World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:11, No:5, 2017

Stackelberg Security Game for Optimizing Security of Federated Internet of Things Platform Instances

Violeta Damjanovic-Behrendt

***Abstract*—**This paper presents an approach for optimal cyber security decisions to protect instances of a federated Internet of Things (IoT) platform in the cloud. The presented solution implements the repeated Stackelberg Security Game (SSG) and a model called Stochastic Human behaviour model with AttRactiveness and Probability weighting (SHARP). SHARP employs the Subjective Utility Quantal Response (SUQR) for formulating a subjective utility function, which is based on the evaluations of alternative solutions during decision-making. We augment the repeated SSG (including SHARP and SUQR) with a reinforced learning algorithm called Naïve Q-Learning. Naïve Q-Learning belongs to the category of active and model-free Machine Learning (ML) techniques in which the agent (either the defender or the attacker) attempts to find an optimal security solution. In this way, we combine GT and ML algorithms for discovering optimal cyber security policies. The proposed security optimization components will be validated in a collaborative cloud platform that is based on the Industrial Internet Reference Architecture (IIRA) and its recently published security model.

***Keywords*—**Security, internet of things, cloud computing, Stackelberg security game, machine learning, Naïve Q-learning.

I. Introduction

THE *more ubiquitous and connected, the more unsafe and vulnerable* – this is a simple rule of thumb in today's connected world in which things, objects, processes, services, cloud bots, and human users need to seamlessly communicate, while performing online tasks of varying complexity.

The Internet of Things (IoT) and Cloud computing bring new challenges to the existing landscape of cyber threats [1]-[4]:

- Security risks of systems and processes are continuously growing (i.e. risks concerning machine working conditions, information related to process performances, maintenance data);
- The privacy of individuals is changing and becoming more vulnerable (i.e. risks related to purchasing preferences, medical records, social attitudes, ethical considerations);
- Risks related to third-party suppliers and vendors are spreading (i.e. risks related to corrupt practices, disruption, data security breaches and espionage, outsourcing risks);
- Security of physical environments, data, applications, etc.

The existing security and privacy mechanisms relying on lightweight cryptography, standard privacy assurance methods and secure protocols, are becoming less effective in the IoT. Trust management approaches are changing with broadening of the IoT business ecosystems, calling for new practices to detect fraudulent certificates and to trust online opinions.

Critical infrastructures such as digital automation systems, manufacturing, the financial sector, etc. are getting more exposed to cybercrime, which results in additional net losses including both direct and indirect costs, reputation damage, and further effects on hundreds of people and companies who find more often their personal or corporate information stolen. Hence, one of the main challenges for cybersecurity researchers and practitioners is to decide to what extent existing approaches are worth integrating into the IoT, and where new IoT protocol designs may better accomplish privacy and security goals, overall [5]. These challenges bring a huge complexity of factors that need to be considered for the IoT and Cloud computing. For example, the top vulnerabilities in Cloud computing include [6], [7]:

- Session ridings (when an attacker steals a user's cookie and continues using the applications for which he/she does not have rights);
- Insecure cryptography that provides a small entropy pool so that the numbers can be computed by brute force;
- Data protection and portability when changing the cloud vendor;
- Cloud provider lock-in (changing to another provider when needed, or combining services provided by various cloud provider);
- Internet dependency.

In this paper, we discuss some common cyber security issues related to the IoT and Cloud computing, and propose a distributed Game Theory (GT) model for ensuring cyber security of multiple instances of a federated platform, residing in the cloud. In section 2, we survey the existing GT approaches for maximizing cyber security in the IoT and in Cloud computing. Here, we consider four categories of GT approaches to Wireless Sensor Networks (WSN) security: (i) preventing Denial of Service (DoS) attacks, (ii) detecting intrusion, (iii) strengthening security, and (iv) detecting coexistence with malicious sensor nodes. In section 3, we summarize the future technological directions in decision support and GT in the IoT and Cloud computing, and identify the Stackelberg Security Games (SSG) and Machine Learning (ML) techniques as our candidate approach for security decision-making. Section 4 describes our decision-support approach to optimizing security in the cloud. The core problem to be addressed in this paper is about ensuring maximum cyber security on a B2B Internet platform where

Violeta Damjanovic-Behrendt is with Salzburg Research Forschugsgesellschaft, Salzburg, Austria (phone: +43-662-2288-427; fax: +43-662-2288-222; e-mail: violeta.damjanovic@salzburgresearch.at).

individual firms can enter into supply chain agreements and enforce private contracts and transactions including data exchange. The context of our work is a European research project under Horizon 2020 programme. Finally, section 5 concludes the paper.

II. State-of-the-art in Game Theory for Optimizing Cybersecurity in the IOT

The problem of optimizing the trade-off between privacy and utility has been discussed in the literature notably in the context of statistical databases [8]-[12]. It is proven that the problem of maximizing privacy under utility constraint, assuming the existence of the prior knowledge, is equivalent to the user's best strategy in a zero-sum game against adaptive adversaries [13]. However, if we want to guarantee a certain level of privacy for the user and to maximize his/her utility, we cannot model the problem as a zero-sum game. One possible solution to this problem, as discussed in [14], involves a GT approach to privacy for designing optimal obfuscation mechanisms against adaptive inference. Such a game is formulated as *a Stackelberg Game* and uses linear programming to solve the identified problem.

Currently, there is a plethora of GT algorithms and experimentations to balance and optimize privacy and security issues. For example, the authors in [15] explore several ways of combining security challenges and GT, i.e. intrusion detection systems (DIS), anonymity and privacy, cryptography, etc. The authors in [16] summarize 29 publications with the focus on the use of GT approaches to formulate problems related to security and energy efficiency. Shen et al. in [17] summarize additional 30 publications on existing GT approaches to strengthen WSN security, which are classified into four categories: (i) preventing DoS attacks, (ii) detecting intrusion, (iii) strengthening security, and (iv) detecting coexistence with malicious sensor nodes.

A. Game Theory Mechanisms for Preventing DoS Attacks

GT mechanisms for preventing DoS attacks in sensor networks are based either on non-cooperative game algorithms [18]-[20], cooperative games [21] or repeated games [22], [23]. For example, the authors in [22] present a protocol based on repeated games, in which there are nodes that agree to forward packets but fail to do it (known as passive DoS). The jamming and anti-jamming attacks are modelled as a zero-sum stochastic game in [24]. Dong et al. in [25] establish an attacking-defending GT model for detecting active DoS attacks, in which the strategy space and payoff matrix describes both the IDS and the malicious nodes.

B. Game Theory Mechanisms for Intrusion Detection

Several GT frameworks for modelling IDS have been presented in literature; for example, the authors in [26] model IDS using a method similar to sampling in communications networks. The authors in [27], [28] analyse the interaction between an attacker and a host-based IDS using a dynamic two-player non-cooperative game. The authors in [29], [30] further discuss the available IDS techniques and model attacks using GT algorithms. They propose a framework for detecting malicious nodes based on a zero-sum approach for nodes in the forward data path. Mohi et al. in [31] model the interaction of nodes in WSN and IDS as a Bayesian game. Michiardi and Molva [32] use cooperative and non-cooperative GT algorithms to develop a reputation-based architecture with the aim to enforce cooperation. Xie et al. in [33] shows that non-cooperative GT algorithms have the potential to improve performances and efficiency of anomaly detection schemes in WSN. The authors in [33] suggest the statistical models to be used over rule-based models as faster and more efficient for hierarchical structures. Qiu et al. in [34] propose an active defence model for WSN based on evolutionary GT. The authors in [35] analyse the cooperation stimulation and security in self-organized WSN under a GT framework.

C. Game Theory Mechanisms for Strengthening Security

GT mechanisms to strengthening security often refer to auction theory [36] and coalitional games [37]. For example, the authors in [36] propose the Secure Auction-based Routing (SAR) protocol, which uses the First-Price auctions to isolate suspicious sensor nodes. Similarly, the authors in [38] propose auction theory to be used to satisfy different users' requests in manufacturing resource models, while the greedy method is used to further search for the optimal bid in the bid set.

In addition, coalitional games establish specific characteristics functions, based on rules such as:

- A sensor node will join a coalition only if it can create more payoff than being alone;
- A coalition will exclude a sensor node if the sensor node cannot benefit the coalition.

These are examples of rules under which the selfish sensor nodes that do not forward others' data packets will hardly be admitted into coalitions because of their poor reputation. With such rules, sensor nodes are forced to participate in a coalition and those that cannot join into any coalitions, are under high suspicion of being interpreted as malicious.

D. Game Theory Mechanisms for Detecting Coexistence with Malicious Sensor Nodes

GT mechanisms for detecting coexistence with malicious sensor nodes use two separated sets of strategies for describing behaviour of the sender and the receiver, with an assumption that one of them is a malicious node and the other is a regular sensor node in WSN [39]. In this case, the overall net utility is calculated based on various combinations of the sender-receiver interaction strategies.

III. Future Directions in Securing the IoT and Cloud Computing

In the IoT, objects and "things" often communicate via Cloud computing servers, which enable the use of a collection of *distributed services, applications, information and infrastructure,* and which are comprised of pools of computing, network, information and storage resources [40]. Cloud computing brings new functionality such as storage and management, business processes execution, etc., to the IoT. In

parallel, it brings new challenges and risks for data security, privacy and trust. As noted in [41], security issues and their solutions in one area are not always directly applicable in others; for example, the security solutions used in ad-hoc networks are similar to those in sensor networks, but the defense mechanisms are not directly applicable for several reasons:

- Public key cryptography used in ad-hoc networks is too expensive to be implemented in sensor networks;
- Symmetric key cryptography protocols from ad-hoc networks are unsuitable for sensor networks.

Cybersecurity challenges related to IoT devices and Cyber Physical Systems (CPSs) affect the entire IoT ecosystem, leading to malfunction of devices and control systems for manufacturing, energy suppliers, implying severe financial losses or, in the worst case, danger to people's lives. The state of the art in the development and implementation of CPSs does not deliver secure software yet. Many security enhancing programming languages have been proposed, but none have had traction in CPSs [42]. For example, some problematic aspects of the existing security enhancing programming languages could be:

- They do not provide support for type checking of data objects passed through interfaces;
- Object types might have attributes, which need to be formulated at the various levels, including the level of interfaces for authentication;
- They are not fast enough for CPSs,
- They neither offer predictable behaviour nor features that significantly enhance security (i.e. update security features).

As stated in [42], more research is needed in areas such as increasing confidence in sensor readings by checking consistency with other sensors and information sources. At the same time, security of service interoperability plays an important role supporting both security and availability of services (and data) through their interoperability. Given the importance of cloud services to the IoT, the challenges related to cloud-to-cloud interoperability and security need to be better explored, too [43]. Some novel approaches for security in cloud computing add more intelligence in the data itself using, i.e. the framework of Trusted Computing (TC) and privacy enhanced business intelligence that implements the encryption of all cloud data via methods such as: searchable (or predicate) encryption [44], homomorphic encryption [45] and private information retrieval (PIR) [46].

Here, we explore the usage of the SSG for formulating distributed strategies in the cloud. As stated in [47], the Stackelberg equilibrium is achieved if and only if the continuous dynamics converge to a fixed point corresponding to the Stackelberg equilibrium, while minimizing the costs. We enhance the SSG model by recording the states and actions of the attackers and the defenders. We also apply Machine Learning (ML) techniques to assist decision-making in network security.

IV. Security Games and Machine Learning for Optimal Distributed Security Decisions

A. Stackelberg Security Games (SSGs) for Distributed Decisions

A SSG is a two-player GT model, which is used to formulate the interaction between the defender and the attacker. In SSG, the defender commits to a strategy *S*, and the attacker optimizes its rewards *REW* according to the defender's action *A* [48]. In SSG, the attacker knows the mixed strategy *S* of the defender, but not the exact action *A* the defender will take in real time. In real world security situations, the defender is often uncertain about the type of the defender, which is considered by the *Bayesian SSG* [48].

In our game, we are focused on repeated interaction scenarios between defenders and attackers in the cloud. Our work follows *Repeated SSG* and a model called *Stochastic* SHARP [49]. SHARP extends the standard *Rationality models in Repeated Stackelberg Games* (BRRSG), by evaluating some alternative aspects of the security interaction, during decision-making [49] such as:

- Success/failure of the opponent's past actions;
- Similarity between exposed and unexposed areas of the surface, and
- Probability weighting function based on the existing human behaviour models.

B. Machine Learning for Decision Support in Network Security

To learn specific values of the attacker's behaviour for each attack, which is necessary to find the optimal decisions on the defender performances, the SHARP model [49] employs the SUQR [50]. SUQR is based on work in behavioural decision-making from 1972 [51], [52], and its main idea is that individuals have their own evaluations of each alternative during decision-making. For example, the subjective evaluations ($eval_1$ ... $eval_n$) encode information about the importance of security attributes as considered either by the defenders or by the attackers.

Here, in order to formulate a Subjective Utility (SU) function, we briefly introduce the necessary notation.

- REW_i^{def} is the defender's reward for selecting action *A* to protect security resource *i*;
- PEN_i^{def} is the defender's penalty for selecting action *A* that will not protect security resource *i*;
- REW_i^{att} is the attacker's reward for targeting security resource *i*, which is not adequately protected;
- PEN_i^{att} is the opponent's penalty for targeting security resource *I*, which is adequately protected.

A SU function of the attacker SU_i^{att} can be defined as a linear combination of three elements: (i) the defender's coverage probability for security resource *i*, (ii) the attacker's reward REW_i^{att} and (iii) the attacker's penalty PEN_i^{att} (1).

$$\mathrm{SU_i^{att}} = \mathrm{eval_1 S_i} + \mathrm{eval_2 REW_i^{att}} + \mathrm{eval_3 PEN_i^{att}} \quad (1)$$

Two alternative approaches to learning the attacker's

behaviour and the defender's performances are given in [53]:

- *Bayesian SUQR*, which implements a Bayesian Stackelberg game with infinite types, and
- *Robust SUQR*, which combines data-driven learning and robust optimization to address settings without sufficient data available to provide a reasonable hypothesis about the distribution of the attack values.

In our approach, in addition to the SHARP and SUQR models from [49], we employ reinforced ML algorithms to complement GT-based optimal security decisions. Reinforced learning is a general-purpose framework for Artificial Intelligence (AI), which similarly to GT, selects specific actions in order to maximize future rewards, and provides learning features like memory, conditional computations, etc. The recent comparison of the efficiency of Q-Learning algorithms (such as Minmax and Naïve Q-Learning) and traditional Markov games, shown that Naïve Q-Learning is promising approach compared to the Markov game and Minmax Q-Learning [54]. In order to solve some remaining limitations, the authors in [54] suggest that it is necessary to further study how to tune the parameters of a Naive Q-Learning algorithm given real data from a series of attacks, which we expect to be one of the core contribution of our mixed GT and ML security optimization.

V. Decision Support for Optimizing Cybersecurity of the Federated IoT Platform Instances

This paper presents our approach to cybersecurity research challenges as defined in the NIMBLE project (H2020 Grant No. 723810), and which combines SSG, SHARP and Naïve Q-Learning in finding the optimal security decisions in the IoT and Cloud computing. The main objective of the NIMBLE project is to create a collaborative and federated platform for industry, manufacturing, business and logistics in Europe. The NIMBLE platform is multi-sided and cloud-based. It includes various end-to-end IoT solutions and devices, used to provide communication and collaboration via cloud-based sector-centric platform instances (Fig. 1).

The main security challenges in NIMBLE include risks at the level of edge devices, gateways and communication, cloud services, and lifecycle management data. The overall architecture is distributed, which requires non-centralized algorithms to be used for computing mixed-strategy equilibria and for translating these equilibria in specific security policies. The security policies vary from one federated platform instance to the other, and by employing SSG, we will enable each platform instance to set its specific "randomization policy" for which the opponent can further choose a "scanning rate" (subjective evaluations of each alternative during decision-making) after observing the "randomization policy". For example, for the platform instance defenders, the trade-off is expected to be between the cost of scanning and protecting the platform nodes, while for the attacker, the trade-off is between the cost of scanning and attacking the real node.

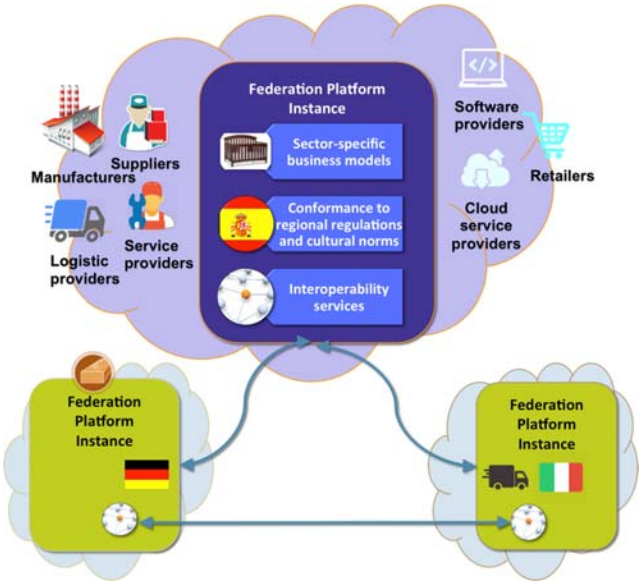

Fig. 1 NIMBLE federated collaboration network with sector-centric platform instances

Employing the SHARP and SUQR models in NIMBLE enables the analysis of the attacker-defender behaviour and learning about their performances (their states and actions). Fig. 2 illustrates the *OPtimization Reinforced learning Architecture (OPRA)*, which will be implemented as a security optimization component in the NIMBLE platform. The OPRA components are inspired by the Google DeepMind's GORILA (General Reinforcement Learning Architecture), a framework for massively distributed reinforcement learning [55].

The OPRA security optimization components include:

- *Platform Instance Defender*: Each defender process contains a replica of repeated SSG model and of the distributed Q Network, which is a Naïve Q-Learning model. Both models, repeated SSG and Q Network complement each other in learning about optimal security decisions in the cloud.
- *Attacker*: Each attacker process contains a replica of repeated SSG model and of the distributed Q Network, which are used in learning about the attacker's behaviour (the outcomes of the attacker's actions on the distributed environment).
- *Distributed Memory* contains records of evaluated states and actions generated by the attacker.
- *Parametrized Policies* receives gradients from the *Platform Instance Defenders*, and iteratively uses these gradients to optimize (update) the parameter vector and to search for an optimal security policy. The optimization is based on a gradient descent algorithm (the Q-Learning algorithm), which iteratively updates the parameters and estimates the gradient based on experience (Fig. 2).

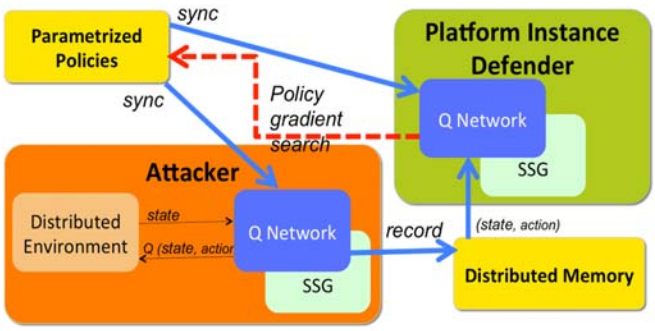

Fig. 2 NIMBLE OPtimization Reinforced learning Architecture (OPRA) based on SSG and Naïve Q-Learning

VI. Conclusion

GT has been proved in the literature and in numerous real world successfully deployed applications as an approach for improving WSN performance objectives caused by the limited capabilities of sensor nodes in terms of computation, communication, and energy (i.e., GT can maximize sensing coverage, extend operation periods, or improve security aspects via adequate mathematical generalization). Furthermore, GT mechanisms can be used to monitor behaviour of sensor nodes and to evaluate reputation of each node based on collected observations, which can be used to predict the future behaviour of nodes in WSN. Similarly to WSN, the distributed environment of the IoT and the Cloud computing can be seen as an experimental playground for distributed strategies for cyber security. Therefore, in this paper, we analyse the background GT approaches to be used for optimal security decisions, which we further complement with Naïve Q-Learning, a reinforced learning algorithm.

Acknowledgment

This research has been funded by the European Commission within the H2020 project NIMBLE (Collaborative Network for Industry, Manufacturing, Business and Logistics in Europe), No. 723810, for the period between 01 October 2016 - 31 September 2019.

References

[1] EY, "Cybersecurity and the Internet of Things. Insights on governance, risk and compliance", March 2015. Online available: https://go.ey.com/1CjIS8f (Last accessed: January 9, 2017)

[2] W.S. Inbarani, C.K.C. Paul, and W.A.J. Jeevakumar, „A Survey on Security Threats and Vulnerabilities in Cloud Computing", International Journal of Scientific & Engineering Research, Volume 4, Issue 3, March 2013.

[3] K. Dahbur, and B. Mohammad, "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing.", International Conference on Intelligent Semantic Web-Services and Applications, (ISWSA '11). ACM, New York, NY, USA, 2011, Online available: http://www.jisajournal.com/content/4/1/5 (Last accessed: January 9, 2017)

[4] M. Ahmed, and M.A. Hossain, "Cloud Computing and Security Issues in the Cloud", IJNSA, Vol.6, No.1, January 2014. Online available: http://airccse.org/journal/nsa/6114nsa03.pdf (Last accessed: January 9, 2017)

[5] R. Roman, P.Najera, and J.Lopez, "Securing the Internet of Things", IEEE Computer, vol.44, pp.51-58, 2011. Online available: http://doi.org/10.1109/MC.2011.291 (Last accessed: January 9, 2017)

[6] V.O. Safonov, Trustworthy Cloud Computing, (1st Ed.), Wiley Publishing, 2016.

[7] M.A. Bamiah, and S.N. Brohi, " Seven Deadly Threats and Vulnerabilities in Cloud Computing," IJAEST, 2011, pp. 87-90. Online: https://www.academia.edu/4877213/Seven_Deadly_Threats_and_Vulnerabilities_in_Cloud_Computing (Last accessed: January 9, 2017)

[8] F. Brunton and H. Nissenbaum, "Vernacular resistance to data collection and analysis: a political theory of obfuscation," First Monday, 16(5), 2011 http://firstmonday.org/article/view/3493/2955 (Last accessed: December 16, 2016)

[9] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," In Proceedings of the 41st annual ACM symposium on Theory of computing, ACM, 2009, pp. 351-360.

[10] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," SIAM Journal on Computing, 41(6), pp. 1673-1693, 2012.

[11] C. Li, M. Hay, V. Rastogi, G. Miklau, and A. McGregor, "Optimizing linear counting queries under differential privacy," In Proceedings of the 29th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of database systems, ACM, 2010, pp 123-134.

[12] S. Ioannidis, A. Montanari, U. Weinsberg, S. Bhagat, N. Fawaz, and N. Taft, "Privacy tradeoffs in predictive analytics," arXiv preprint arXiv: 1403.8084, 2014.

[13] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, „Protecting location privacy: optimal strategy against localization attacks," In Proceedings of the ACM conference on Computer and Communication Security, 2012.

[14] R. Shokri, „Privacy games: optimal user-centric data obfuscation," In Proceedings on Privacy Enhancing Technologies 2015 (2), pp. 1-17.

[15] M.H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J.-P. Hubaux, „Game Theory meets network security and privacy," ACM Computing Surveys, 45(3), 2012.

[16] R. Machado and S. Tekinay, „A survey of Game Theoretic approaches in Wireless Sensor Network," Computer Network 2008, 52, pp. 3047–3061.

[17] S. Shen, G. Yue, Q. Cao, and F. Yu,"A survey of Game Theory in Wireless Sensor Networks security," Journal of Networks, 2011, 6, pp. 521–532.

[18] A. Agah, K. Basu, S.K. and Das, "Enforcing security for prevention of DoS attack in Wireless Sensor Networks using economic modelling," In Proceedings of 2005 IEEE International Conference on Mobile Adhoc and Sensor Systems, Washington, DC, USA, 2005.

[19] A. Agah, K. Basu, S.K. and Das, „Preventing DoS attack in Sensor Networks: A Game Theoretic approach," In Proceedings of 2005 IEEE International Conference on Communications, South Korea, 2005.

[20] Y.E. Sagduyu, and A. Ephremides, „A Game Theoretic analysis of Denial of Service attacks in Wireless Random Access," Wireless Networks, 2009, 15, pp. 651–666.

[21] A. Agah, S.K. Das, and K. Basu, „A Game Theory based approach for security in Wireless Sensor Networks," In Proceedings of 2004 23rd IEEE International Performance, Computing and Communications Conference, Phoenix, AZ, USA, pp. 15–17, 2004.

[22] A. Agah, and S.K. Das, "Preventing DoS Attacks in Wireless Sensor Networks: A repeated Game Theory approach," Int. J. Network Security 2007, 5, pp. 145–153.

[23] L. Yang, D. Mu, and X. Cai, "Preventing dropping packets attack in Sensor Networks: a Game Theory approach," Wuhan Univ. J. Nat. Sci. 2008, 13, pp. 631–635.

[24] H. Li, L. Lai, and R.C. Qiu, „A Denial-of-Service jamming game for remote state monitoring in Smart Grid," In Proceedings of 2011 45th Annual Conference on Information Sciences and Systems, MD, USA.

[25] R. Dong, L. Liu, J. Liu, and X. Xu, „Intrusion Detection System based on payoff matrix for Wireless Sensor Networks," In Proceedings of 2009 3rd International Conference on Genetic and Evolutionary Computing (WGEC 2009), Guilin, China, 2009.

[26] M. Kodialam and T. V. Lakshman, "Detecting network intrusions via sampling: a Game Theoretic approach," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE INFOCOMM 2003, (Piscataway, NJ, USA), pp. 1880--1889, IEEE Press, 2003.

[27] T. Alpacan and T. Basar,"A Game Theoretic approach to decision and analysis in network intrusion detection," in Proceedings of 43rd IEEE Conference on Decision and Control, (USA), IEEE Press, 2004.

[28] A. Patcha and J.M. Park," A Game Theoretic formulation for intrusion detection in mobile ad hoc networks," International Journal of Network

Security, Vol.2, No.2, PP.131–137, 2006.
[29] Y.B. Reddy, "A Game Theory approach to detect malicious nodes in Wireless Sensor Networks," In Proceedings of 2009 3rd International Conference on Sensor Technologies and Applications, Greece, 18–23, 2009.
[30] Y.B. Reddy, and S. Srivathsan, S., "Game Theory model for selective forward attacks in Wireless Sensor Networks," In Proceedings of 2009 17th Mediterranean Conference on Control and Automation (MED), Thessaloniki, Greece, 2009.
[31] M. Mohi, A., Movaghar, and P.A., Zadeh, "Bayesian game approach for preventing DoS attacks in Wireless Sensor Networks." In Proceedings of 2009 WRI International Conference on Communications and Mobile Computing, Kunming, China, 2009.
[32] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in Proceedings of the 6th IFIP Communications and Multimedia Security Conference, 2002.
[33] M. Xie, S. Han, B. Tian, and S. Parvin, "Anomaly detection in Wireless Sensor Networks: a survey," Journal of Network Computing Applications, 2011, 34, pp. 1302–1325.
[34] Y. Qiu, Z. Chen, and L. Xu, "Active defence model of Wireless Sensor Networks based on evolutionary Game Theory," In Proceedings of 2010 6th International Conference on Wireless Communications, Networking and Mobile Computing, Chengdu, China, 2010.
[35] J. Chen, and R. Du, "Fault tolerance and security in forwarding packets using Game Theory," In Proceedings of the 2009 International Conference on Multimedia Information Networking and Security (MINES 2009), Hubei, China, 2009.
[36] A. Agah, K. Basu, and S. K. Das, "Security enforcement in Wireless Sensor Networks: a framework based on non-cooperative games," Pervasive and Mobile Computing, vol. 2, Apr. 2006, pp. 137-158.
[37] X. Li and M. R. Lyu, "A novel coalitional game model for security issues in wireless networks," In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM 2008), 2008, pp. 1- 6.
[38] Y. Wang, J. Bo, and G. Li, "Research on cloud manufacturing resource allocation in distributed computing environment", Int. Journal of Grid Distribution Computing, Vol. 8, No. 3, 2015.
[39] W. Wang, M. Chatterjee, and K. Kwiat, "Coexistence with malicious nodes: a Game Theoretic approach," In Proc. International Conference on Game Theory for Networks (GameNets '09), 2009, pp. 277-286.
[40] Cloud Security Alliance (CSA)'s Security Guidance for Critical Areas of Focus in Cloud Computing (2009), CSA.
[41] C. Karlof and D. Wagner,"Secure routing in Wireless Sensor Networks: attacks and countermeasures," Ad Hoc Networks, Volume 1, Issue 2, pp. 293-315.
[42] S. Peisert, et al., "Designed-In security for Cyber-Physical Systems," IEEE Computer and Reliability Societies. September/October 2014.
[43] Internet Society, "The Internet of Things: an overview," Understanding the Issues and Challenges of a More Connected World, 2015.
[44] Song, D., Wagner, D., and Perrig, A., "Practical techniques for searches on encrypted data," In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, California, USA, pp. 44-55, 2000.
[45] Gentry, C., "Fully homomorphic encryption using ideal lattices," In Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09), pp. 169-178, Maryland, USA, 2009.
[46] Chor, B., Kushilevitz, E., Goldreich, O., and Sudan, M., "Private Information Retrieval," Journal of ACM (JACM), Vol 45, No 9, pp. 965-981, 1998.
[47] P. Lee, A. Clark, B. Alomair, L. Bushnell, and R. Poovendran, "Passivity-based distributed strategies for stochastic Stackelberg Security Games," *IEEE Conference on Game and Decision Theory for Security (GameSec)*, 2015.
[48] P. Paruchuri, J. P. Pearce, J. Marecki, M. Tambe, F. Ordonez, and S. Kraus, "Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg Games," In Proceedings of the 7th International Joint Conference on Autonomous Agents and Multiagent Systems – Vol. 2, AAMAS, pp. 895–902, 2008.
[49] D. Kar, F. Fang, F. D. Fave, N. Sintov, and M. Tambe, „A Game of Thrones: when human behaviour models compete in repeated Stackelberg Security Games," In International Conference on Autonomous Agents and Multiagent Systems (AAMAS), 2015.
[50] T. H. Nguyen, R. Yang, A. Azaria, S. Kraus, and M. Tambe, "Analyzing the effectiveness of adversary modelling in security games," In AAAI, 2013.
[51] Savage, L. J., The Foundations of Statistics. Dover Publications. 1972.
[52] Fischhoff, B., Goitein, B. and Shapira, Z., "Subjective utility function: a model of decision-making," American Society of Information Science 32(5): 391–399. 1981.
[53] W. Haskell, D. Kar, F. Fang, M. Tambe, S. Cheung, and E. Denicola. "Robust protection of fisheries with compass," In Innovative Applications of Artificial Intelligence (IAAI), 2014.
[54] K. Chung, C. A. Kamhoua, K. A. Kwiat, Z. T. Kalbarczyk and R. K. Iyer, "Game Theory with learning for cyber security monitoring," 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE), Orlando, FL, 2016, pp. 1-8.
[55] A. Nair, et al., "Massively parallel methods for Deep Reinforcement learning," Deep Learning Workshop, International Conference on Machine Learning, Lille, France, 2015. Online available: https://arxiv.org/abs/1507.04296 (Last accessed: December 16, 2016)