BRIEFING NOTES

BN-80-The role of AI-Aug2021

PUBLIC AND DEFENCE POLICY CHALLENGES AND INNOVATIONS ON ARTIFICIAL INTELLIGENCE, AUTONOMOUS SYSTEMS, AND CYBERSECURITY

PART 3: REINFORCEMENT LEARNING ALGORITHMS FOR CYBERSECURITY AND MILITARY DEFENSE APPLICATIONS

Authors: Neshat Elhami Fard [1], Rastko R. Selmic [2], and Kash Khorasani [2]

[1] Graduate student, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

[2] Professor, Department of Electrical and Computer Engineering, Concordia University, Montreal, Canada

SUMMARY

- The intelligence that is appeared in man-made machines and enables devices to imitate individual behavior is artificial intelligence (AI). AI is different from human and animal intelligence, which is intertwined with consciousness and emotion [1].
- As a subset of the AI method, machine learning (ML) is used to improve the performance of machines, utilizing statistical techniques [2].
- Both reinforcement learning (RL) algorithms, which are used to solve numerous sequential decision-making problems, as well as deep learning (DL) methods, which utilizes multi-layer neural networks (NN) for learning large volumes of data, are subsets of ML [3], [4], [5].
- Deep reinforcement learning (DRL) is a combination of DL and RL (two subdivisions of ML) and has been established to overcome the high-dimensional problems that RL algorithms encounter [6].
- Using RL and DRL, intelligent devices, similar to humans who learn from experiences, can learn from the actions they take at every time step t [7].

CONTEXT

- One of the RL and DRL applications is in the cyber-physical systems (CPS) for cyber-attacks as well as cyber-attack detection [8], [9]. Since the CPS models have infinite state space, conventional methods such as cross-entropy are not suitable for detecting their defects. In this regard, RL and especially DRL algorithms have many simulations runs and are superior to other methods in identifying CPS models' weaknesses containing software complexities [8].

CONSIDERATIONS

- According to research conducted by the authors of [10]– [12], the cybersecurity tasks using DRL algorithms are intrusion detection, malware detection, privacy and security [7]. For instance, in [10], utilizing a labeled dataset, a proper application of various DRL algorithms is offered to intrusion detection.
- Thee specifications of this application are applying fast and straightforward NN to implement the classifier, using a flexible reward function, requiring a simple update of parameters in case of online learning [10].
- In [11] a DRL architecture including an adaptive cloud infrastructure is proposed to intrusion detection. The characteristics of this DRL cloud intrusion detection

system are being robust to modern attacks plus being able to maintain a balance between high accuracy and less false positive rate [11].

- In [12] a DRL algorithm based on deep Q-networks is presented to decrease the malware attacks in order to preserve the reliability, privacy, and security of the entire system.
- Various researches have been conducted to introduce and develop defense strategies and applications using RL and DRL algorithms.
- The authors of [13] have proposed three defense strategies using DRL. In detail, this method increases the accuracy of the DRL agent that is attacked, and in contrast, takes defensive positions against the dynamic actor-critic DRL jamming attacker. These strategies are: utilizing a proportional integral derivative (PID) control, using an imitation attacker, and developing orthogonal policies.
- Another application of RL and DRL algorithms is in the multi-agent systems' defense and attack. In multi-agent systems, cooperation between agents is a vital issue that all agents must be able to learn efficient approaches to accomplish their goals. RL and DRL algorithms can be a solution to the cooperation problem. In this regard, the authors of [14] have presented a multi-agent deep deterministic policy gradient (MADDPG) algorithm for multi-agent defense and attack, containing rule-based attackers and DRL-based attackers accompanying DRL-based defense agents.

BACKGROUND

- Cybernetics, during the development of automated range finders for anti-aircraft guns, was introduced by Norbert Wiener in 1940 [15]–[17]. Wiener's proposed method is an adjustment and re-adjustment cycle by aircraft and an antiaircraft gun. In this method, several observations are made to predict the future position of a flying aircraft during tracking, and the anti-aircraft gun's actions should be added to the previous forecast [16].
- Both cyberspace and CPS terms are derived from cybernetics, respectively. In this regard, cyberspace was introduced by William Gibson in 1982 [18]. Regarding Gibson's theory, cyberspace is a real non-space world identified by the ability to present virtually as well as interact with individuals through icons, waypoints, and AI [19].
- Afterward and for the first time, Helen Gill proposed the concept of CPS at the United States National Science Foundation (NSF) CPS workshop in 2006 [18], [20]. As a computer system, the mechanisms of a CPS are controlled and monitored using computer-based algorithms [21].

- RL usage has flourished over the past decade. For the first time, Thorndike [22] introduced RL in 1898 with an experiment on cat's behavior, and other researchers have further supplemented it over the years [23], [24]. In general, an agent of an RL algorithm receives a state from the environment and performs an action related to the received state at time step t. Then, according to the completed action, the agent gets a reward in the form of compensation or punishment from the environment at time t + 1. The goal of the algorithm is to maximize the cumulative reward [25].
- DL, which was introduced by Walter Pitts and Warren McCulloch in 1943, is a computer model based on the human brain's NN and is a combination of algorithms and mathematics [26]. Finally, in 2015, DRL was developed by integration of DL architectures, and RL algorithms [6].

NEXT STEPS

- The next report will review the cybersecurity and defense applications of AI, especially RL and DRL algorithms in CPS. For further familiarization with these systems, various types of cyber-attacks and cyber-attack detection will introduce. Besides, the RL and DRL algorithms for cyber-attack detection will present. Finally, the RL and DRL algorithms for defense applications will study.

REFERENCES

[1] "Artificial intelligencehttps://en.wikipedia.org/wiki/Artificialintelligence, April 2021.
[2] S. Singh, "Cousins of artificial intelligence," https://towardsdatascience.com/cousins-of-artificial intelligencedda4edc27b55, May 2018.
[3] N. Elhami Fard and R. R. Selmic, "Effects of an immediate reward on consensus behavior of a leaderless multi-agent reinforcement learning system," in 2021 IEEE International Conference on Systems, Man and Cybernetics (SMC), Submitted to IEEE, 2021.
[4] T. T. Nguyen, N. D. Nguyen, and S. Nahavandi, "Deep reinforcement learning for multiagent systems: A review of challenges, solutions, and applications," IEEE Transactions on Cybernetics, 2020.
[5] H. Ji, O. Alfarraj, and A. Tolba, "Artificial intelligence-empowered edge of vehicles: architecture, enabling technologies, and applications," IEEE Access, vol. 8, pp. 61 020–61 034, 2020.
[6] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski, et al., "Human-level control through deep reinforcement learning," nature, vol. 518, no. 7540, pp. 529–533, 2015.
[7] I. H. Sarker, "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective," SN Computer Science, vol. 2, no. 3, pp. 1–16, 2021.
[8] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," arXiv preprint arXiv:1906.05799, 2019.
[9] S. Mahdavifar and A. A. Ghorbani, "Application of deep learning to cybersecurity: A survey," Neurocomputing, vol. 347, pp. 149–176, 2019.
[10] M. Lopez-Martin, B. Carro, and A. Sanchez-Esguevillas, "Application of deep reinforcement learning to intrusion detection for supervised problems," Expert Systems with Applications, vol. 141, p. 112963, 2020.
[11] K. Sethi, R. Kumar, N. Prajapati, and P. Bera, "Deep reinforcement learning based intrusion detection system for cloud infrastructure," in 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS). IEEE, 2020, pp. 1–6.
[12] P. M. Shakeel, S. Baskar, V. S. Dhulipala, S. Mishra, and M. M. Jaber, "Maintaining security and privacy in health care system using learning based deep-q-networks," Journal of medical systems, vol. 42, no. 10, pp. 1–10, 2018.
[13] F. Wang, C. Zhong, M. C. Gursoy, and S. Velipasalar, "Defense strategies against adversarial jamming attacks via deep reinforcement learning," in 2020 54th annual conference on information sciences and systems (CISS). IEEE, 2020, pp. 1–6.
[14] L. Huang, M. Fu, H. Qu, S. Wang, and S. Hu, "A deep reinforcement learning-based method applied for solving multi-agent defense and attack problems," Expert Systems with Applications, vol. 176, p. 114896, 2021.
[15] J. Von Neumann, N. Wiener, and S. J. Heims, From mathematics to the technologies of life and death. MIT press, 1981.

[16] N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine. MIT press, 2019.
[17] N. Elhami Fard, K. Haratiannejadi, R. R. Selmic, and K. Khorasani, "Public policy challenges, regulations, oversight, technical, and ethical considerations for autonomous systems: A survey," Submitted to: IEEE Technology and Society Magazine, 2021.
[18] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," Sensors, vol. 15, no. 3, pp. 4837–4869, 2015.
[19] V. Fourkas, "What is cyberspace," Spatial Development Research Unit, Department of Urban and Regional Planning and Development, Aristotle University of Thessalonica, 2004.
[20] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," Computers in Industry, vol. 100, pp. 212–223, 2018.
[21] "Cyber-physical system," https://en.wikipedia.org/wiki/Cyber-physicalsystem, May 2021.
[22] E. L. Thorndike, "Animal intelligence: An experimental study of the associate processes in animals." American Psychologist, vol. 53, no. 10, p. 1125, 1998.
[23] M. L. Minsky, Theory of neural-analog reinforcement systems and its application to the brain model problem. Princeton University., 1954.
[24] A. H. Klopf, Brain function and adaptive systems: a heterostatic theory. Air Force Cambridge Research Laboratories, Air Force Systems Command, 1972, no. 133.
[25] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction . MIT press Cambridge, 2018.
[26] K. D. Foote, "A brief history of deep learning," https://www.dataversity.net/brief-history-deep-learning/, February 2017. [27] K. Kersandt, "Deep reinforcement learning as control method for autonomous uavs," Master's thesis, Universitat Politecnica de Catalunya, ` 2018.