Security-Policy NET Nexus of Emerging Technologies

BRIEFING NOTES

# BN-81-The role of AI-Aug2021

PUBLIC AND DEFENCE POLICY CHALLENGES AND INNOVATIONS ON ARTIFICIAL INTELLIGENCE, AUTONOMOUS SYSTEMS, AND CYBERSECURITY PART 4: 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

- Cyber-physical systems (CPS), including various specifications, e.g., complexity, dynamic variability, and heterogeneity, consists of cyber and physical subsystems [1].
- Different types of CPS are smart grids, smart transportation, and smart industrial manufacturing [1].
- One of the advantages of RL algorithms is that they can make accurate decisions automatically in an unknown environment by trial and error experiences [1]. Therefore, they can be used for cyber-attack or cyber-defense applications.

CONTEXT

- In the next section, various cyber-attacks related to the RL and DRL algorithms for different cyber-physical systems are studied.
- Afterward, in the second section, the different types of cyber-attack detection and defense applications are designed and developed by RL and DRL algorithms for diverse cyber-physical systems.

CONSIDERATIONS

Reinforcement Learning Algorithms for Cyber-Attack

- **Cyber-attacks on Smart Grids**
    - Since the smart grid is a complex cyber-physical system as an electrical network, including various operations and energy measures, multiple attacks and any other disruption in this network can destroy the entire system in a little while. In this regard, different attacks must be detected early to operate securely and reliably on a smart grid [2]. Due to the system's vulnerability to malicious attacks [3], we first examine these types of attacks in each smart grid. Malicious attacks are divided into two categories: physical attacks and cyber-attacks [4]. In physical attacks, the components of the power grids are physically attacked and destroyed. These components include transformers, transmitters and transmission lines, generators, etc. The topology and data processing modules located in the control center can effortlessly detect this type of attack. Besides, cyber-attack occurs differently. Unlike physical attacks, power grid components are not physically attacked, but the measurable data transmitted in the supervisory control and data acquisition (SCADA) system is modified and compromised. A well-thought-out and sophisticated cyber-attack can manipulate the topology and data processing modules and completely mislead or disrupt the performance of the control center [5].

  - The authors of [3] have proposed a coordinated topology attack to overload a critical line by misleading the control center. In this method, both physical attack and cyber-attack are integrated and perform the coordinated topology attacks using DRL algorithms. The function of the coordinated topology attack is: first, the physical attack interrupts the transmission line; second, it hides the cut line signal in the cyber layer (masking a physical tripped line); finally, it generates a fake cut-off signal for the following transmission line (creating a cyber tripped line). There are two types of DRL algorithms in this introduced method: one to determine the attack strategy in order to overload a critical transmission line; another one to select minimal attack resources in order to inject the cyber attack with limited attack resources. For the aforementioned coordinated topology attack, the utilized DRL algorithms are based on deep Q-learning algorithms [3].

Cyber-attacks on Software-defined Networking

  - ``Software-defined networking (SDN) is a network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software applications [6]." When the SDN's cyber-defense system is defined using RL algorithms, the cyber attacker tries to modify or destroy the training process in the RL algorithm. In this case, the cyber attacker can perform this change and destruction in two ways: forging and changing part or all of the reward signal; manipulation and modification of some states received from the environment [7]. Therefore, when the defender agent receives the wrong state and reward from the environment, it will not perform the correct optimal action in response to the inaccurate data. As a result, the purpose of the system is delayed or compromised.

Cyber-attacks on any Cyber-physical System

  - The major challenge that sometimes arises is related to the unknown cyber-attacks that threaten any cyber-physical system. One advantage of known cyber-attacks over unknown one is that by recognizing the type of attack and realizing how to model it, the cyber-defence can be provided more reliably and securely. Since the type of unknown cyber-attacks is undetectable, there must be an online cyber-attack detection method that can perform an optimal and effective defence strategy in an instant according to the existing conditions. In this regard, it is better to use learning-based methods (e.g., RL algorithms) against these attacks to learn the existing conditions in real-time and defend online.

Reinforcement Learning Algorithms for Cyber-attack Detection and Defense Applications:

Cyber-defense of Smart Grids

  - Considering the problems that occur for smart grids due to the discussed issues related to cyber-attacks, raised in Section~\ref{section1}, the authors of [2] have formulated an online cyber-attack detection problem as a partially observable

Markov decision process (POMDP). Afterward, as a solution, they have provided a robust online detection algorithm based on model-free RL algorithms for detecting cyber-attacks that target a smart grid. The RL cyber-attack detection algorithm incorporates two stages: learning; and online detection. In the learning stage, the defender is trained by the SARSA algorithm (a model-free RL algorithm) and learns a Q-table. In the online detection stage, the learned Q-table in the learning stage is utilized to select the action with the lowest expected future cost. Since the proposed algorithm by the authors of [2] is general, it is widely able to detect any type of attack, both known and unknown instances.

- **Cyber-defense of Software-Defined Networking:**
    - The authors of [7] have proposed a RL method to have a suitable autonomous cyber-defense against attackers who intend to infiltrate and propagate throughout the entire SDN and compromise critical network servers. In this proposed method, it is supposed to train two diverse RL agents. One agent is based on double deep Q-networks (DDQN) RL algorithm to isolate the agents and preserve them from attacks. Another agent is the asynchronous advantage actor-critic (A3C) RL algorithm to keep nodes uncompromised and reachable from the critical server. Therefore, this method allows RL agents to perform sub-optimal actions despite the presence of attacks on RL algorithms [7].
- **Cyber-defense of any Cyber-physical System:**
    - The authors of [8] have introduced and developed a particular type of optimal online cyber-defence to combat unknown cyber-attacks in a cyber-physical system. The steps of the suggested method are: an innovative cyber-state dynamics has been created that can assess the effects of the current cyber-attack as well as the defence strategy efficiently and dynamically in real-time; since cyber-attack is unknown and there is not sufficient information about the cyber-state dynamics, to provide an optimal cyber-defence, an actor-critic NN architecture has been proposed to learn the optimal online cyber-defence strategy effectively; finally, a novel actor-critic DRL algorithm has been implemented to improve the proposed method [8].

NEXT STEPS

- The following report will continue the above topics, and it 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] X. Liu, H. Xu, W. Liao, and W. Yu, "Reinforcement learning for cyber-physical systems," in 2019 IEEE International Conference on Industrial Internet (ICII). IEEE, 2019, pp. 318–327.

[2] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5174–5185, 2018.

[3] Z. Wang, H. He, Z. Wan, and Y. Sun, "Coordinated topology attacks in smart grid using deep reinforcement learning," IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 1407–1415, 2020.

[4] X. Li, X. Liang, R. Lu, X. Shen, X. Lin, and H. Zhu, "Securing smart grid: cyber attacks, counter measures, and challenges," IEEE Communications Magazine, vol. 50, no. 8, pp. 38–45, 2012.

[5] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1362–1370, 2012.

[6] "What is sdn?" https://www.ciena.com/insights/what-is/What-Is-SDN.html, June 2021.

[7] Y. Han, B. I. Rubinstein, T. Abraham, T. Alpcan, O. De Vel, S. Erfani, D. Hubczenko, C. Leckie, and P. Montague, "Reinforcement learning for autonomous defence in software defined networking," in International Conference on Decision and Game Theory for Security. Springer, 2018,pp. 145–165.

[8] M. Feng and H. Xu, "Deep reinforcement learning based optimal defense for cyber-physical system in presence of unknown cyber-attack," in 2017 IEEE Symposium Series on Computational Intelligence (SSCI). IEEE, 2017, pp. 1–8.