Jie CHEN, Dandan WU, Ruiyun XIE, 2023. Artificial intelligence algorithms for cyberspace security applications: a technological and status review. *Frontiers of Information Technology & Electronic Engineering*, 24(8):1117-1142. https://doi.org/10.1631/FITEE.2200314

Artificial intelligence algorithms for cyberspace security applications: a technological and status review

Key words: Artificial intelligence (AI); Machine learning (ML); Deep learning (DL); Optimization algorithm; Hybrid algorithm; Cyberspace security

Corresponding author: Jie CHEN
E-mail: chenjie1900@mail.nwpu.edu.cn

ORCID: https://orcid.org/0000-0002-5643-193X

Introduction

This work presents a comprehensive review of AI technology articles for cyberspace security applications, mainly from 2017 to 2022.
This survey is unique in that it covers a wide range of AI algorithms in three kinds of cyberspace security applications, not only machine learning (ML) and deep learning (DL), but also optimization algorithms.

- Introduction of the main algorithms that are widely used in the area of AI
- Applications of AI algorithms to cyberspace security
- Comparison and discussion
- Future problems and challenges

Hightlight

This review is particularly comprehensive because it includes the comprehensive AI algorithms in cyberspace security issue applications not only for intrusion detection but also for assessment and defense decision-making:

1. The research material has the characteristics of timeliness, authority, and universality. More than 150 articles were collected, especially from 2011 to 2022. Most of them are indexed by Web of Science, and the authors are influential scholars in the fields of AI and cyberspace security around the world. Among them, 19.70% are from Elsevier journals, 6.58% are from Springer journals, 26.40% are from IEEE journals, and 25% are from conferences.

Hightlight

2. The research problems include difficult problems and active directions in the field of network security. This review studies and analyzes three specific technical problems that need to be solved urgently in the field of cyberspace security, including network attack detection, security situation assessment, and network security defense strategy optimization. In each direction, AI algorithms are classified as ML, DL, or optimization algorithm, and are sorted and analyzed from the aspects of algorithms, datasets, simulation, and comparative experiments, even advantages and disadvantages.
3. Through omni-directional, multi-dimensional, and detailed research, the potential advantages of AI algorithms in solving specific problems in the field of network security are statistically analyzed. It shows the current development trends of technologies and applications, the hot issues, and the focuses of different countries in the field of network security.

Research methods

1. We describe the different AI algorithms used to solve cyberspace security issues, including intrusion detection, prediction and evaluation of the security situation, and generating and optimizing strategies.
2. In each direction, with a specific focus on the latest approaches in ML, DL, and some popular optimization algorithms, the characteristics of the algorithmic models, performance results, datasets, potential benefits, and limitations are analyzed, and some of the existing challenges are highlighted.

Research methods

Fig. 1 shows the relationship between the proportion of the number of papers and the country that the first affiliation belongs to from 2017 to 2022. It can be seen that China pays the highest attention to cyberspace security. China's papers account for 47.62% and USA 14.29%.

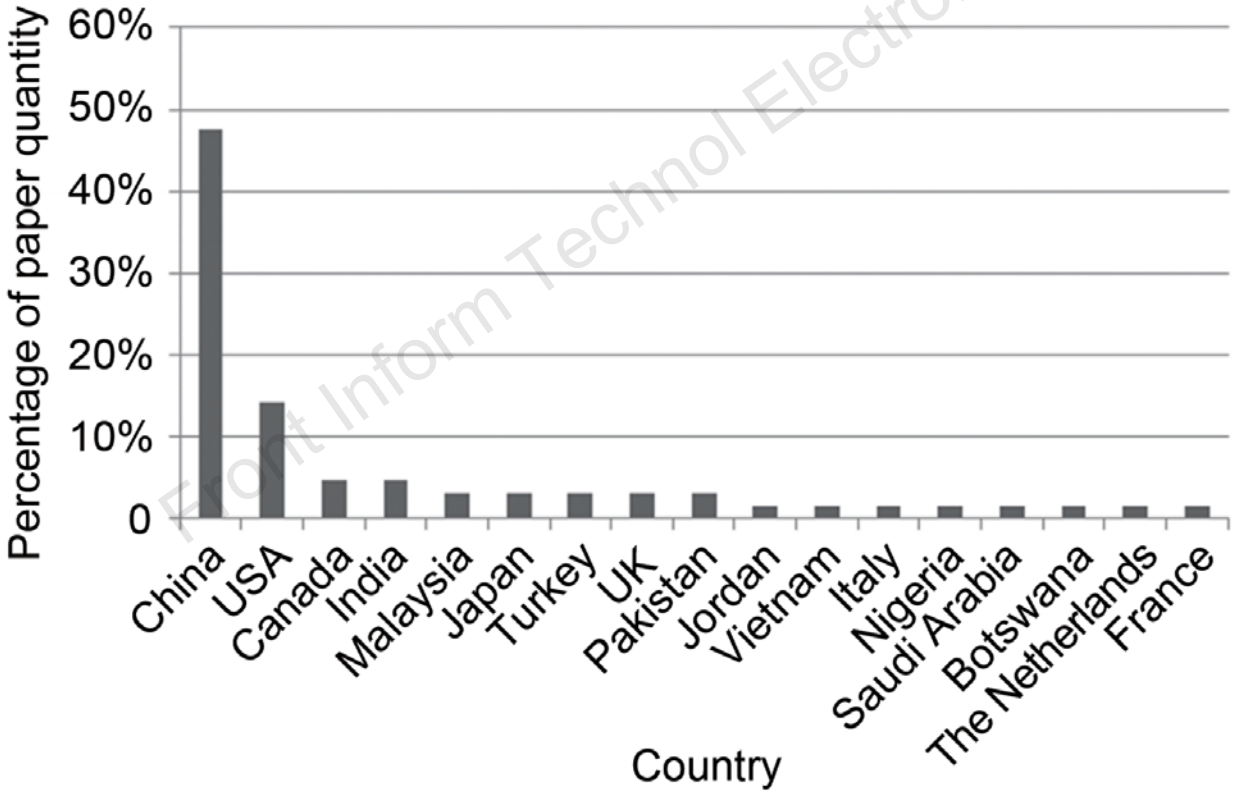


Fig. 1 Analysis of research situation in different countries

Research methods

Fig. 2 shows that there are six countries that pay high attention to the security issues in the three types of cyberspace. Among them, China's attention level is the highest, especially on the issue of network situation assessment, and the attention level reaches 90%. In contrast, USA pays more attention to defense decision optimization.

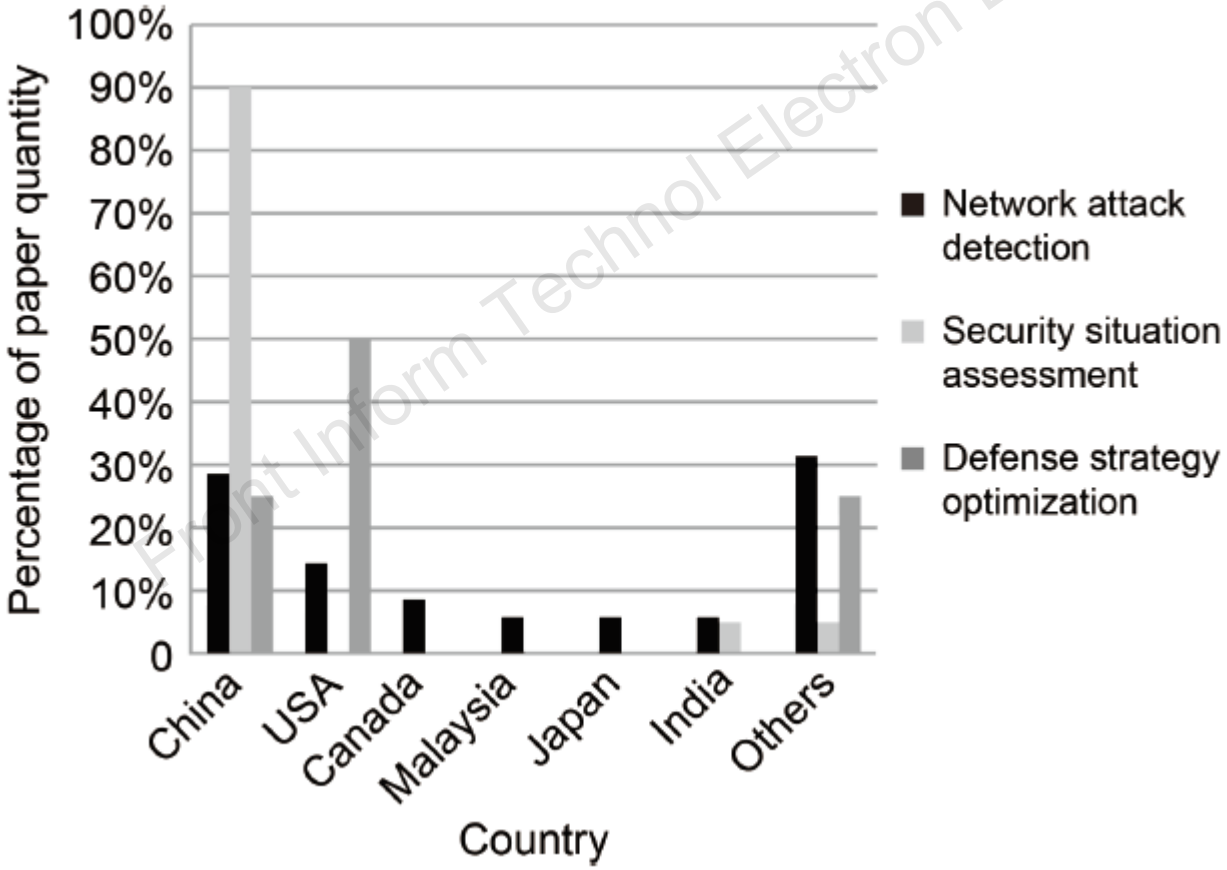
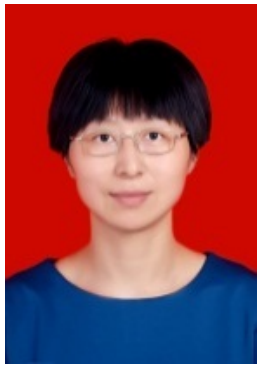


Fig. 2 Analysis of research directions in different countries

Future directions

1. The latest technical exploration indicates that AI algorithms are playing an increasingly important role in guaranteeing cyberspace security, not only developing security ability with good performance in intrusion detection and defense evaluation, but also providing new algorithm design ideas for researchers to explore cyberspace security defense decision-making methods.
2. Network attack detection is an important area in the application of AI technology.
3. In the past six years, Chinese researchers have conducted much research on the credibility assessment and prediction of the security situation, publishing 90% of the papers.
4. The research on the optimization of network security defense strategy was conducted mainly by researchers in USA, with the swarm intelligence (SI) optimization algorithm, and the game theory and deep reinforcement learning (DRL) algorithm for solving the optimization problem of the network security defense strategy.
5. Future work should consider human guidance and some new questions raised by AI algorithms.



Jie CHEN received the BS degree in computer science and technology from Chongqing University of Computer Science, China, in 1999, and received the MS degree in electronic and communication engineering from Sichuan University, China, in 2006. She is currently pursuing the PhD degree in School of Cybersecurity of Northwestern Polytechnical University. She is a researcher-level senior engineer in China Electronics Technology Network Information Security Co., Ltd. Her current research interests include cyberspace security, network defense architecture, and AI algorithms.

Dandan WU received the Postgraduate degree in school of Mechano-Electronic Engineering of Xidian University, Xi'an, China, in 2014. She is a senior engineer in China Electronics Technology Network Information Security Co., Ltd. Her current research interests include cyberspace security and deep learning.

Ruiyun XIE is an associate professor and doctoral supervisor at the Northwestern Polytechnical University. He is a researcher-level senior engineer in China Electronics Technology Network Information Security Co., Ltd. His current research interests include cyberspace security and network confrontation.