Key Problems and Solutions of the Application of Artificial Intelligence Technology

Guangxia Zhou(✉)

Science and Technology on Information Systems Engineering Laboratory,
Nanjing 210007, China
zgx8086@163.com

Abstract. Google's AlphaGo shocked the world by easily defeating Korean Go player Lee Shi-shi, thus setting off a new upsurge of artificial intelligence research and application. Currently, artificial intelligence technology is developing at a speed beyond imagination, and it has become the core and key to the leap-forward development of every industry. However, application of artificial intelligence technology also encounters many problems. Key problems of military application of artificial intelligence are analyzed emphatically, and solutions to those problems are introduced, as a reference to further research.

Keywords: Artificial intelligence technology · Machine learning · Autonomous learning · Deep learning

1 Introduction

In March 2016, AlphaGo, developed by DeepMind, a subsidiary of Google, shocked the world by easily defeating Korean Go player Lee Shi-shi, thus setting off a new upsurge of artificial intelligence (AI) research and application. AI technology is developing at a speed beyond imagination, and it has become the core and key to implement leap-forward development in every industry. The military, of course, is no exception and has higher expectation. In military, AI is a revolutionary and enabling technology capable of improving mission tasks from intelligence gathering to situation predicting, decision-making and autonomous unmanned combat. Thus, world's military powers have continuously strengthened their research and application of AI and expect to seize the strategic commanding heights. However, compared with the civil application, the application of AI in military has great particularity, such as the restraint of war ethics. This paper does not discuss such issues, but only the related technical problems of AI military application. These problems include data, security, credibility, etc., which hinder the military application of AI technology. These problems must be solved before AI technology can be widely used in the military. Through the analysis of the exploration of AI military application at home and aboard, solutions to the above problems are suggested, as a reference to further research.

Q. Liang et al. (Eds.): *Artificial Intelligence in China*, LNEE 572, pp. 407–414, 2020.
https://doi.org/10.1007/978-981-15-0187-6_48

2 Problem Analysis

Generally speaking, the main problems of the application of AI technology in military are as follows:

First is data. Data is the lifeblood of AI. Without dataset, AI has become a passive water. Learning has neither object nor verification basis. Data problems include three aspects: Firstly, the problem of data source—in peacetime, operational data mainly comes from the aggregate of daily duty, live exercise, training and other ways. However, these aggregates are far from enough to effectively support machine learning. Even the USA, which has fought the most war in the world in recent years, has the richest aggregate of battlefield data in the world, but its Defense Innovation Unit (DIU) still thinks that the key to restricting the application of AI in the military is that there are too few machine learning datasets available in a short and strong competed environment, which makes it difficult for AI systems to carry out tasks effectively in the complicated and competed environment [1]; secondly, the problem of data comprehensiveness—the rapid development of AI technology is mainly due to the continuous development of deep learning system. By deep learning, a large amount of information can be inputted into the computer to allow deep learning system to learn and analyze data. However, the data used to train deep learning system is not comprehensive although it is constantly improving. For example, when using AI system to pick out fruits, people train visual recognition algorithms by learning a large number of image databases. The purpose is usually to identify the “natural” appearance of fruits. However, compared with the bright photographs of intact fruits, there are relatively few pictures of rotten fruits. And unlike humans, AI systems tend not to calculate or ignore them, while the human brain tends to pay attention to these abnormal groups and react strongly to them [2]. In military application scenarios, this situation is even more serious; and thirdly, the problem of data annotation—current machine learning systems acquire a large amount of data through sample learning, which has been independently labeled by analysts to generate the required output. With the development of the system, deep neural network (DNN) has become the latest technology in machine learning model. DNN can provide power for tasks such as machine translation and speech or object recognition with higher accuracy. However, training DNN requires a lot of labeling data. The process of accumulating and labeling a large amount of information is expensive and time-consuming. In addition to the challenge of accumulating labeled data, most machine learning models are fragile and vulnerable to collapse when their operating environments change slightly. For example, in speech recognition systems, if the acoustic environment or the sensor of the microphone changes, it may be necessary to retrain on a completely new dataset. The time and effort required to adjust or modify the model are almost equivalent to recreating the model.

Second is the problem of autonomous learning. At present, AI takes machine learning technology as its core and relies on huge dataset. However, the battlefield environment is complicated and changeable, the competition is violent, the situation is changing rapidly, full of fog and accident, and the AI system cannot predict all possible factors or scenarios when it is developed. In order to carry out its mission under any circumstances, the military AI system must have the ability of self-learning and quickly react to sudden and extreme situations on the battlefield.

Third is the problem of security. AI system is facing many threats in battlefield, including physical damage and cyber attack. Comparing with the hard damage caused by physical attack, the soft damage caused by cyber attack may be more serious and more difficult to prevent. The US's "Resilient Military Systems and Advanced Cyber Threat" describes the situation of missile control system being hacked and may be directed against own troops [3]. The software nature of AI system determines the inevitability of cyber attack. This is because the intelligent function of AI system comes from the software composed of various branch logics, variable tables and parameter tables [4]. The more complex the task and the more diverse the environment, the higher the complexity of the software, the wider the scope involved, the more vulnerabilities and weaknesses, the greater the possibility of being broken.

Fourth is the problem of credibility. In civil AI products, as long as the algorithm is effective, the others are not so important. How to allocate drivers and determine routes for Uber? How does Google generate search results? How does Tesla's autopilot work? Many users are not particularly concerned [5]. In military applications, commanders often need to know the reasons for AI system decision-making, because of the problems of life and death, war ethics and so on, before they can make up their minds. But AI cannot explain its thoughts and actions to commanders, and commanders cannot fully understand the decision-making process of AI system and cannot distinguish the logic behind a specific action of AI system, which often leads commanders to distrust the decision-making and action made by intelligent system. Therefore, credibility is the key to the wide application of AI system in battlefield.

3 Solution Analysis

In view of the above problems in the application of AI in military, through the analysis of the research status at home and aboard, especially the USA, solutions to the above problems are suggested as follows.

3.1 Using War Games to Simulate, Generate and Collect Data to Solve Data Source Problems

Game AI has developed rapidly in recent years. AI has defeated humans in most games, including Atari, StarCraft, Dota and so on. The rapid development of intelligent game technology has attracted the attention of the USA and taken a series of related measures. At present, the US Marine Corps University has been experimenting with the "Athena" deduction tool, a simulation and deduction platform dedicated to training, education and testing future AI applications [6]. Using Athena's war game, an air assault task can be planned to control the interception position to support amphibious landing. The game requires the user to complete the planning process when talking to the voice assistant. The program will prompt defensive forms, definitions of different tactical tasks and related historical cases. As the game progresses, an AI application captures data, compares the user's use of cover and range crossing areas, then evaluates the user's performance based on other data and records these data into a database on the combat methods of US military professionals. Finally, Athena evaluates the data and provides constructive suggestions for users, comparing their performance with that of top-level users.

Through this game environment, the USA seeks competent commanders and obtains the data needed to build future AI applications. Once enough data is available, Athena can simulate modern military operations and propose new tactics.

Athena provides a test platform for exploring how to integrate AI into military decision-making process. Using war games to observe how military experts make decisions, benchmark data is established for testing a series of applications that enhance warfighter judgment.

3.2 Explore a New Learning Algorithm to Reduce the Dataset Needed for Model Training and Solve the Problem of Data Annotation

In order to reduce the cost and time associated with training and adjusting machine learning models, DARPA launched the project of Learning with Less Labels (LwLL) [7]. Through the LwLL project, DARPA will study new learning algorithms to greatly reduce the dataset for model training or updating. This project aims to make the process of training machine learning model more efficient. DARPA said that through the LwLL project, the dataset needed to build a model will be reduced by six orders of magnitude or more, and the label precedents used to label the model will be adjusted from millions to hundreds; that is, a million images are needed to train a system now, and only one image or about 100 label precedents will be needed in the future.

To achieve this goal, the LwLL project will explore two technical areas. The first technology area focuses on building efficient learning and adaptive learning algorithms. The main approaches are innovation in meta-learning, transfer learning, active learning, K-shot learning and supervised/unsupervised adaptation. The second technical area explores the normative description of machine learning problems, including the difficulty of decision-making and the real complexity of the data used to make decisions. In this regard, DARPA said that it is difficult to assess the efficiency of building machine learning systems or the basic limitations of the accuracy level of the model. Through LwLL project, we hope to find the theoretical limit of machine learning possibilities and use this theory to promote system development and enhance capabilities.

3.3 Enhancing AI System's Autonomous Learning and Environmental Adaptability by Bionics

At present, AI takes machine learning technology as its core and relies on huge data support. But the real world is full of contingency, and programmers cannot predict all possible factors or situations. When these machine learning systems encounter special situations that are not included in programs and databases, they will be at a loss. If we want to expand the capability of machine learning system in this new environment, we must stop its service and retrain it with additional data, but this method relies on human intervention and is inefficient. In contrast, biological systems can conduct independent training, learn from past experience and adapt to the accumulated knowledge even in the face of a new environment. From here we can see that even the most advanced AI systems at this stage are still far from adaptive biological intelligence. In 2017, DARPA launched a project called Lifelong Learning Machines (L2M) [8].

The learning mechanism proposed by L2M does not need to provide the system with a large number of knowledge sets about applications as it does now. It needs limited domain knowledge and methods to start its behavior and learning. L2M tries to apply biological learning mechanism to machine learning system, breaking the dependence of existing machine learning system on pre-programming and training samples, so that artificial intelligence system, like biological system, can make decisions based on experience. Even in the new situation without experience and training before, it can also make scientific decisions quickly according to "experience" accumulated in "life" and improve its operation. Active autonomy enhances the ability to adapt to the environment. The L2M project will use the principles of computer science and biological learning to build learning paradigms and evolutionary networks, and continue learning through external data and internal goals. At the same time, L2M project will set the limit of system capability and build a security mechanism for AI system.

3.4 Setting Up Machine Commonsense Research to Enhance Reasoning Ability of AI System

Common sense is a basic ability of human beings to perceive and understand the world. Typical AI systems lack a general understanding of how the physical world works, a basic understanding of human motivation and behavior, and a general understanding of things like adults. The lack of common sense hinders the AI system's understanding of the world, its natural communication with humans, its rational behavior in unpredictable situations and its learning of new experiences.

At present, in all machine learning applications, machine reasoning is relatively narrow and highly specialized. Researchers must train and program AI systems for each situation, but commonsense reasoning is still missing. To this end, in 2018, DARPA launched a project called Machine Common Sense (MCS) [9]. The MCS project will explore the latest developments in cognitive understanding, natural language processing, in-depth learning and other areas of artificial intelligence research to find answers to commonsense questions.

The MCS project plans to adopt two strategies to develop two different kinds of commonsense services and to design a special evaluation method for the two services. The technical area of research includes the following three aspects: First is the foundation of human common sense, learning experience to build computational models that can simulate human perception of objects (intuitive physics), agents (intentional actors) and locations (space navigation). These computational models will assess and identify cognitive development milestones in developmental psychology research and the literature to determine their learning effectiveness at three levels (prediction/expectation, empirical learning and problem solving). The second is the basic experimental environment of human common sense. The basic test environment of human common sense will be used when testing the research results in the field of technology, i.e., the foundation of human common sense. Third, there is a wide range of common sense. Learn from online reading to construct answers to natural language questions about commonsense phenomena and image-based questions. The service will simulate the general knowledge of American adults in 2018 and will be judged through the benchmark test of the Allen Institute of Artificial Intelligence (AI2). DARPA predicts that researchers will use manual construction, information extraction, machine learning, crowd sourcing and other computational methods to build the knowledge base.

3.5 Developing Cyber Resilience to Actively Address the Security Problem of AI System

In October 2016, the USA released two strategic documents related to the development of artificial intelligence, the National Strategic Plan for Research and Development of Artificial Intelligence and Preparing for the Future of Artificial Intelligence. In the area of AI security, the National AI Research and Development Strategic Plan of the USA emphasizes the new challenges that traditional network security may bring in AI environment [10]. It is considered that AI systems embedded in key systems must be durable and secure to cope with large-scale deliberate network attacks. It is believed that the application of AI system will bring some new and unique threats. At the same time, the report also emphasizes that AI systems may eventually adopt “cyclic self-improvement”; that is, a large number of software modifications will be made by the software itself, rather than by human programmers. In order to ensure the security of self-modifying systems, additional research is needed to develop self-monitoring frameworks such as checking the consistency of the system’s behavior through the original goal of the designer or proven value frameworks that can resist self-modifying.

In the Report “Summer Study on Autonomy” released by the Defense Science Board of the United States Department of Defense, the answer to the cyber security problem of intelligent military applications is to enhance the cyber resilience of intelligent systems [4].

Cyber resilience can effectively deal with the security problems of AI system because the focus of cyber resilience shifts from preventing cyber attacks to minimizing the impact of cyber attacks. It does not seek to establish a perfect system to deal with all kinds of incidents, including anti-attack. Instead, it adopts a series of technical means to improve the system’s self-active protection ability, so that the key tasks of the system can still be carried out normally in the “toxic carrier” environment, under attack or even under partial control, and maintain the normal function of the system, so as to take the next step. The measures lay the foundation [3].

In January 2013, the US Department of Defense released the report “Resilient Military System and Advanced Cyber Threat,” which proposed the construction of resilient military system. In August 2014, the US Air Force issued a “Cyber Resilience” research guide, which calls for accelerating the research of resilience mechanism and key technologies, survival and recovery of core mission functions, cyber deception, cyber agility, resilience and agility of embedded systems [11].

3.6 Revealing the Transparency of AI Decision-Making and Enhancing Credibility by Improving the Interpretability of AI System

Interpretability of AI systems has become a key obstacle to human–computer cooperation. Explainable Artificial Intelligence (especially explainable machine learning) will be indispensable if we want human beings to understand, trust and effectively manage the new generation of AI systems. To this end, in October 2016, DARPA launched the Explainable Artificial Intelligence (XAI) project [12]. The goal is to establish new or improved machine learning technology, generate explainable models and integrate effective interpretation technology to enable end users to understand, trust and effectively manage future AI systems. Through this project, the new machine learning system will be able to explain its own logic principles, describe its own advantages and disadvantages, and explain future behavior.

Explainable AI faces three challenges: how to generate explainable models, how to design interpretive interfaces and how to understand users' psychological needs for effective interpretation.

In response to the first challenge, the project will develop a series of new or improved machine learning technologies to generate more interpretable models; in response to the second challenge, it hopes to integrate the latest human–computer interaction technologies (such as visualization, language understanding, language generation and session management) with new principles, strategies and technologies for effective interpretation; in response to the third challenge, the project will plan to summarize, expand and apply current psychological theories of interpretation.

At present, the project has achieved some results. At the IJCAI/ECAI 2018 Workshop on Explainable Artificial Intelligence (XAI) conference held in July 2018, several papers funded by the project were published, including depth adaptive programming through reward decomposition interpretation, natural language interpretation of visual question and answer using scene diagrams and visual attention generation, finite state representation of learning cycle strategy network, etc.

4 Conclusion

Artificial intelligence technology has shown good application prospects in all walks of life and has become the core and key to achieve leap-forward development of every industry. Military field is no exception. According to the characteristics of military field, four key problems of AI application in military are analyzed and summarized, including data problem, autonomous learning problem, security problem and credibility problem. For each of these problems, through the analysis and summary of domestic and foreign research, the corresponding solutions are introduced, which can provide reference to related research.

References

1. Jin X (2017) Status and development of intelligent command and control. Command Inf Syst Technol 8(4):10–18
2. Vanian J (2018) Artificial intelligence is too easy to be corrupted by bad examples, what should we do? http://www.fortunechina.com/business/c/2018–07/12/content_311635.htm. Cited 6 May 2019
3. Zhou GX (2017) US military cyber deterrence and cyber resilience. Command Inf Syst Technol 8(5):76–80
4. Defense Science Board (2016) Summer study on autonomy, Washington
5. Mclemore C, Lauzen H (2018) The dawn of artificial intelligence in naval warfare. https://nosi.org/2018/06/16/the-dawn-of-artificial-intelligence-in-naval-warfare/?shared=email&msg=fail. Cited 6 May 2019
6. Jensen B, Cuomo S, Whyte C, Wargaming with ATHENA: how to make militaries smarter, faster, and more efficient with artificial intelligence. http://www.warontherocks.com Cited 6 May 2019
7. DARPA (2018) Learning with Less Labels (LwLL), Arlington, Virginia
8. DARPA (2017) Lifelong Learning Machines (L2M), Arlington, Virginia
9. DARPA (2018) Machine Common Sense (MCS), Arlington, Virginia
10. Wang YP (2017) Information security in artificial intelligence strategy. Secrecy Sci Technol 11:27–30
11. Lan YS, Zhou GX, Wang H, Yi K (2015) Construction mechanism and implementation of resilient command information systems. J Command Control 1(3):284–291
12. DARPA (2016) Explainable Artificial Intelligence (XAI), Arlington, Virginia