CENTRE FOR LAND WARFARE STUDIES

ISSUE BRIEF

No. 119 December 2017

Fathoms of Deep Learning

Col **Sandeep Tyagi** is a Senior Fellow at the Centre for Land Warfare Studies, New Delhi.

What is Deep Learning?

Deep learning, also referred to as hierarchical or deep structured learning, is nothing but a technique that teaches machines and computers 'how to learn by example', which we humans can do naturally and intuitively. This is part of a broader scheme called machine learning methods, a term coined by Arthur Samuel[1] in 1959 while he was with IBM. Deep learning is an area of machine neural networks, artificial intelligence, graphical modelling, optimisation, pattern recognition and signal processing.[2]

Theoretically, deep learning has been around for over 46 years: in 1971, Ivakhnenko trained an 8-layer neural network using the Group Method of Data Handling (GMDH) algorithm.[3] However, it is manifesting now in a big way primarily because of improved processing power and big data. The same is discussed below.

- **Processing / Computing Power**: The computer industry as well as the consumers

Key Points

1. Deep learning is a subset of machine learning and a method for teaching machines/computers to 'learn by example'.
2. Big data and exponentially improved processing power has made deep learning possible in the present times.
3. Deep learning, in most cases, employs the Neural Network Architecture (NNA) also referred to as Deep Neural Networks (DNN).
4. Deep learning has a number of defence applications to include Intelligence, Surveillance, Reconnaissance (ISR), cyber security, cognitive Electronic Warfare (EW), Anti-Ballistic Missile (ABM) defence, autonomous mobile robotics and 3D simulation.
5. The USA and China have made remarkable progress in the deep learning and Artificial Intelligence (AI) domains and are considered to be the global leaders.

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an autonomous think-tank dealing with national security and conceptual aspects of land warfare, including conventional and sub-conventional conflict and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

Website: www.claws.in Contact us: landwarfare@gmail.com

Fathoms of ...

used to refer to the Central Processing Unit (CPU) as the processor, starting the early 1960s. CPUs performed the basic arithmetic, logical and input/output operations as specified by the programme instructions. Subsequently, CPUs evolved over the years, travelling through stages of transistors, small scale integration, and large scale integration to the microprocessor. However, in the year 1999, M/S Nvidia came up with the world's first Graphical Processing Unit (GPU)[4] when it launched the Nvdia GeForce 256 processor. The GPUs have only grown better since then and have acquired great processing powers. Currently, Nvdia and AMD have achieved the 16/14 nm process# respectively. In research done by Indigo, it was found that while training a deep learning neural network (discussed subsequently in this brief), GPUs can be 250 times faster than CPUs. That's a difference between one day of training and almost 8 months and 10 days of training.[5] This has had a salutary effect on the deep learning industry.

- **Big Data**: For the purpose of deep learning extremely large data sets are required to train the system. Earlier it was not possible, however, we are currently going through a global data boom. In the year 2013, *Science Daily* claimed that 90 percent of the world's data was generated in the last two years.[6] This data could be both labelled and unlabelled. Labelled data refers to data (unlabelled) to which meaningful tag(s) have been added to make that data informative. This can be done by tasking humans to identify what is seen in a photograph/video, heard in an audio or read in a text file. This, in turn, can be further applied to unlabelled data using a machine/deep learning model and likely label(s) can be guessed therein.

Fig 1[10]

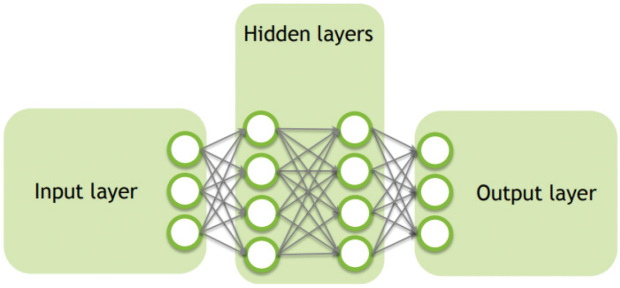


Fig 2

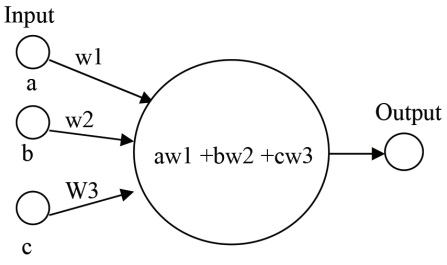
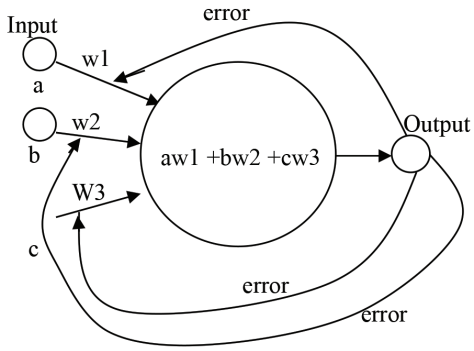


Fig 3



The naming of technology node as "x nm" comes from the International Technology Roadmap for Semiconductors (ITRS). One nanometre (nm) is one billionth of a metre. The smallest commercial chips now use 10nm technology. This simply means that the smaller the chip, more powerful it becomes in its computing power.

How Does it Work?

The Neural Network Architecture (NNA) is what most of the deep learning systems employ. In fact, this is the reason sometimes these are referred to as Deep Neural Networks (DNN). Artificial Neural Networks (ANN), an idea going back to the 1950s, seeks to mimic the way the brain absorbs information and learns from it.[7] The term "deep" usually refers to the number of hidden layers in the neural network. Traditional neural networks only contain 2-3 hidden layers, while deep networks can have as many as 150.[8] A neural network then looks something like Fig 1.

This involves providing some input, conducting some calculation and producing an output – it is that simple! Without giving it too much mathematical treatment, it can simply be understood by the fact that each input node (the green circles in the input layer in the figure above and an artificial neuron referred to as the node hereinafter) are providing some input to each node in the first hidden layer (connected by a link which has an adaptive weight assigned to it – Fig 2). So the input of each node is multiplied by the adaptive weight of the link and then summed up at each node in the hidden layer. This then is passed on to the second hidden layer, and so on. It is quite easily done by the computer as it is nothing but matrix multiplication being executed by a learning algorithm which is the forte of GPUs. Based on the results at the output layer, the error is calculated and is back propagated in proportion of the adaptive weights of the link and the calculations are done again (Fig 3). This is exactly where the learning happens. Thus, the weights are tweaked and iterations done till such time a final result is achieved which is closest to the correct result i.e. with errors minimised. To adequately sum up the learning process described above, a definition of learning coined by T.M. Mitchell can be quoted here, "A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E".[9] Therefore, based on the type of data set being used, deep learning may be classified as under:

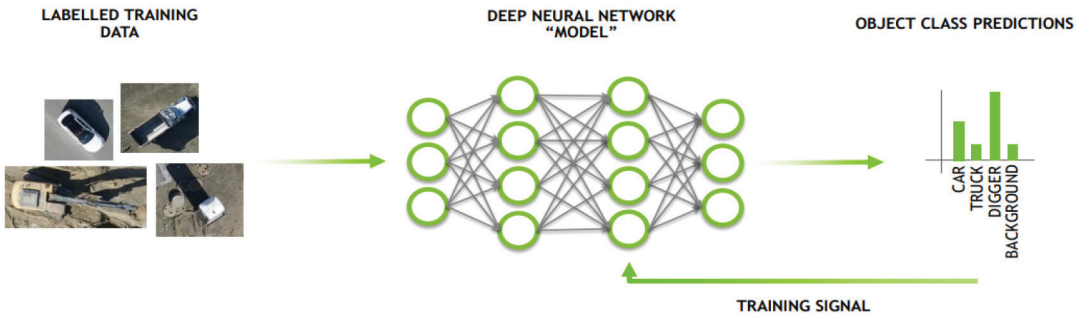
- **Supervised Learning**: This category of learning, presents the data set with a set of parameters. Further, labels or values are provided for each parameter. This mapping of parameters to labels/values is where the useful information is encoded. Once 'trained', the algorithm is expected to locate the mapping from the parameters of fresh data sets to their correct labels or values.

- **Unsupervised Learning**: In unsupervised learning meaningful parameters of the data are extracted in the absence of labels or values and the system learns on the go.

- **Reinforcement Learning**: Here an interaction takes place between a real/simulated environment and the deep learning system. This interaction provides feedback between the learning system and the interaction experience, thus, improving the result obtained.

Deep learning can be applied to any form of data available, be it photographs, videos, audio files or texts. All that is required is a large amount of data (the bigger, the data set, the better), a deep learning model and lots of processing power. This system, thus, created is capable of improving itself and producing astonishing results! It can be summed up as depicted pictorially in Fig 4.

Fig 4 Deep Learning Process



Source: Nvidia. Recent Advances in Deep Learning, Webinar August 2016[10]

Such a deep learning system allows leveraging large volumes of images in which different categories of objects, for example, vehicles, buildings or weapon platforms are labelled and could be used for training. In practice, this resulted in the ANNs detecting and identifying objects with astonishing accuracy. Microsoft's 152-layer neural network, nearly five times deeper than the next best system, correctly classified images within 1,000 pre-defined categories more than 96 percent of the time![11]

Deep Learning's Applications in Defence

- **Intelligence, Surveillance and Reconnaissance (ISR):** The detection and identification features of deep learning systems lend themselves readily for ISR functions. In addition to facial recognition, the ANNs are capable of recognising speech, language dialects, and actions in a video or even a piece of terrain, utilising aerial pictures taken by aircraft, Unmanned Aerial Vehicles (UAVs) or satellites. *"The amount of video data produced annually by UAVs alone is in the petabyte range, and growing rapidly. Full exploitation of this information is a major challenge. Human observation and analysis of ISR assets is essential, but the training of humans is both expensive and time-consuming. Human performance also varies due to individuals' capabilities and training, fatigue, boredom, and human attentional capacity; one response to this situation is to employ machines …"according to the US Defence Advanced Research Projects Agency (DARPA).*[12] Thus, ANN provides a major force multiplier to the commanders to monitor areas and persons of interest, track them in real time, and initiate actions on 'as required' basis. This technique can also be used to categorise an area as safe or unsafe for troops [post a Chemical, Biological, Radiological, Nuclear (CBRN) strike, for example] using various available techniques providing training parameters to the ANNs. Attempts have also been made to use this as an anti-camouflage measure to detect tanks in foliage, etc. High Power Embedded Computing (HPEC) is also playing a major role in ISR functions. HPEC applications seek to embed supercomputer-like performance in a relatively small, rugged, and embedded form factor in applications that can compromise neither on performance nor on Size, Weight, and Power Consumption (SWaP).[13]

- **Cyber Security:** ANNs can be the key to cyber security and the instrument of choice to detect malware and intrusions. Refer to Fig 5 and 6.

Fig 5

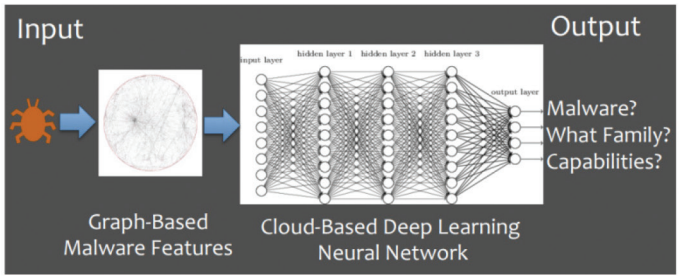
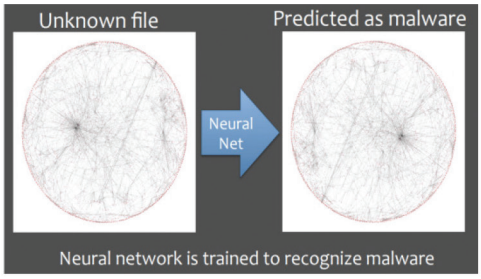


Fig 6



Source: Deep Machine Learning Meets Cybersecurity University of Delaware2017[14]

Presently, malware is being propagated exponentially with over 100,000 malware content being created every hour.[15] It is, therefore, impossible to handle this malware tsunami manually and requires ANNs to keep track of these and predict the kind of damage these are capable of causing. There are two issues that need to be addressed for developing a deep learning counter-measure for the malware. These are: correct parameter selection from the network traffic data set for anomaly detection and generation of sufficient labelled traffic data set from real networks for training the ANNs.

- **Cognitive Electronic Warfare (EW):** The Electronic Counter-Counter-Measures (ECCM) being employed by communication systems and radars have become increasingly sophisticated and can change various characteristics of the transmission continuously. This then makes it that much more difficult for the jammers and spoofers to jam or spoof the Electro-Magnetic (EM) radiations. DARPA is already working on developing an adaptive Electronic Counter-Measure (ECM) system which can use ANNs to learn from these radiations in real time and alter the point of attack of the ECM platforms accordingly.[16] This cognitive Electronic Warfare (EW) effort began in 2010 and is broken into two parts: Adaptive Radar Counter-measures (ARC) and Behavioural Learning for Adaptive Electronic Warfare (BLADE). The two tracks exist because of the differing ways of thwarting an enemy's radar and its communications.[17]

- **Anti-Ballistic Missile (ABM) Defence:** ABM defence systems all over the world are confronted with the challenges of increasingly sophisticated missiles and warheads, including Multiple Independently Targeted Reentry Vehicles (MIRVs). It is a general belief that the best way to counter a ballistic missile both spatially and temporally is when the missile is in its boost phase. This, then, of necessity, requires successful detection, tracking and identification of the hostile missile/launch. This demands multiple sensors on the ground, sea and space to include radars, electro-optical and infrared sensors and an algorithm to fuse these inputs while also accounting for missing, noisy, or corrupted data, and predict the next event. ANNs are being employed to help develop such a system.[18]

- **Autonomous Mobile Robotic Applications:** Together with the HPEC described above, mobile robotic applications are achieving remarkable feats. Driverless cars/combat vehicles, UAVs and robots are all employing ANNs to assess the situation in real time and initiate the desired and required actions accordingly. The employment of such systems is limited only by the user's imagination.

... Deep Learning

- **3-Dimensional Simulation:** There are occasions when limited data is available for a particular mission scenario to include terrain and hostile activities. In such a case, there is a constraint on how ANNs can be employed, in the absence of a large enough data set. In such a case, however, simulated vehicle mounted camera environment and depth data (similar to what one finds in video games) may be generated and then mixed with the limited real world data to simulate the desired scenario. This boot-strapping of the simulated data with the real world data has been found to be quite successful for training ANN models, with the additional benefit of simulating those environments or scenarios which may never be encountered. A dream come true for trainers!

Deep Learning: Important Developments in the World

A lot of development is being undertaken by various nations in the field of deep learning. The more remarkable ones are discussed below:

- **USA:** In November 2014, the then US Secretary of Defence Chuck Hagel announced a new defence innovation initiative, which included the third offset strategy. Hagel said, "This new initiative is an ambitious department-wide effort to identify and invest in innovative ways to sustain and advance America's military dominance for the 21st century.[19] This strategy includes a number of technological components, including deep learning. Also, DARPA is actively pursuing programmes such as High Assurance Cyber Military Systems (HACMS) and cognitive EW which involve deep learning extensively.

- **China:** China is performing extremely well in the field of deep learning. The Chinese government is investing heavily in such technologies and claims that its military and other companies would be leading the world in the field of Artificial Intelligence (AI) by the year 2030.[20] This seems quite possible going by the performance of the Chinese at ImageNet 2017 (ImageNet or Large Scale Visual Recognition Challenge, has emerged as an influential event in the AI research community to track the latest advances in image recognition systems).[21] This year's competition saw top results for the closely-monitored image classification challenge producing an error rate of only 2.25 percent from a Chinese team. Another event presenting the challenge for image recognition based strictly on real world data using smartphone cameras called WebVision, found the top performer to be the Shenzhen-based Malong Technologies. Malong achieved a 94.78 percent accuracy rate in classifying the web images.[22] The Chinese government has created a National Laboratory of Deep Learning[23] and experts believe that this would eventually lead to China surpassing the US in the field of AI.

Deep Learning in India

India has a lot of catching up to do in this field! Despite having all the ingredients available such as trained manpower, a vibrant start-up ecosystem and robust Information Technology (IT) industry, India is still trying to find its feet in the domain of deep learning. This was affirmed by Vishal Dhupar, Managing Director of NVIDIA (South Asia), in an interview given in 2016 to YourStory.[24] Some seminars, training workshops and conferences which have been conducted or are planned to be conducted in deep learning, however, there are no signs of a notable government initiative in this fast expanding and vital technology field.

Conclusion

The sheer volume of data being generated commonly referred to as big data demands analysis at an unprecedented velocity. The conventional computing systems cannot keep up with this and are passé. Be it in the commercial or the military domain, as discussed in this brief, deep learning ignited AI is clearly the future!

Notes

1. "Machine Learning", available at https://en.wikipedia.org/wiki/Machine_learning, retrieved on December 08, 2017.
2. Dr ND Lewis, "Deep Learning Made Easy," with R A Gentle Introduction to Data Science, p. 6.
3. Adrian Carrio, Carlos Sampedro, Alejandro Rodriguez-Ramos, and Pascual Campoy, Review Article, "A Review of Deep Learning Methods and Applications for Unmanned Aerial Vehicles," *Journal of Sensors,* 2017, available at https://www.hindawi.com/journals/js/2017/3296874/, retrieved on December 11, 2017.
4. "Nvidia Launches the World's First Graphics Processing Unit: GeForce 256," available at http://www.nvidia.com/object/IO_20020111_5424.html, retrieved on December 09, 2017.
5. "Graphics Processing Unit", available at https://en.wikipedia.org/wiki/Graphics_processing_unit, retrieved on December 09, 2017.
6. "Big Data, for Better or Worse: 90% of World's Data Generated Over Last Two Years," May 22, 2013, available at https://www.sciencedaily.com/releases/2013/05/130522085217.htm, retrieved on December 09, 2017.
7. John Markoff, "Scientists See Promise in Deep-Learning Programs," *The New York Times*, November 23, 2012.
8. "What Is Deep Learning? 3 Things You Need to Know," available at https://www.mathworks.com/discovery /deep-learning.html, retrieved on December 08, 2017.
9. TM Mitchell, *Machine Learning* (Burr Ridge, Ill, USA: McGraw Hill, 1997), Vol. 45(37), ch 1, p.2.
10. Barker Jon, "Recent Advances in Deep Learning for Defence," June 2016, Webinar. Available at http://on-demand.gputechconf.com/gtc/2016/webinar/deep-learning-for-defense-webinar.mp4, retrieved on December 10, 2017.
11. Nvidia, "From the Frontline: How Deep Learning Plays Critical Role in Military Problem-Solving," available at https://blogs.nvidia.com/blog/2016/06/29/deep-learning-6/, retrieved on December 11, 2017.
12. "Deep Learning Neural Networks (DNN) Transforming Google Search, Object Recognition, Face Detection and Autonomous Military Systems", International Defence Security and Technology (IDST), June 28, 2017, available on http://idstch.com/home5/international-defence-security-and-technology/technology/ict/deep-learning-neural-networks-dnn-have-enabled-machines-to-match-human-vision-skills/, retrieved on December 11, 2017.
13. John Keller, "The Future of High-Performance Embedded Computing," August 11, 2014, available at http://www.militaryaerospace.com/articles/print/volume-25/issue-8/technology-focus/the-future-of-high-performance-embedded-computing.html, retrieved on December 11, 2017.
14. "Deep Machine Learning Meets Cybersecurity University of Delaware, 2017, available at https://www.eecis. udel.edu/~cavazos/cisc850-spring2017/Lecture-01b.pdf, retrieved on December 11, 2017.
15. Ibid.
16. Brian Wang, "DARPA Applying Artificial Intelligence for Realtime Cognitive Electronic Warfare," September 17, 2016, available at https://www.nextbigfuture.com/2016/09/darpa-applying-artificial-intelligence.html, retrieved on December 11, 2017.
17. Ibid.
18. "Exo Analytic Solutions, Robust Classification through Deep Learning and Dynamic Multi-Entity Bayesian Reasoning," available at https://exoanalytic.com/2016/01/01/robust-classification-through-deep-learning-and-dynamic-multi-entity-bayesian-reasoning/, retrieved on December 11, 2017.

19. "US Administration Identifies Disruptive Technologies, Doctrinal Innovation and Nuclear Modernization Under Third Offset Strategy to Sustain America's Military Dominance for the 21st Century," available at http://idstch.com/home5/international-defence-security-and-technology/geopolitics/uss-third-offset-strategy -to-sustain-and-advance-americas-military-dominance-for-the-21st-century/, retrieved on December 12, 2017.
20. Aaron Tilley, "China's Rise in the Global AI Race Emerges as it Takes Over the Final ImageNet Competition," July 31, 2017, available at https://www.forbes.com/sites/aarontilley/2017/07/31/china-ai-imagenet/ #50adb8c2170a, retrieved on December 12, 2017.
21. Ibid.
22. Ibid.
23. Meng Jing, "China's First 'Deep Learning Lab' Intensifies Challenge to US in Artificial Intelligence Race," available at http://www.scmp.com/tech/china-tech/article/2072692/chinas-first-deep-learning-lab-intensifies-challenge-us-artificial, retrieved on December 12, 2017.
24. "With the Rise of Deep Learning and AI, India has Great Opportunity," says NVIDIA's Vishal Dhupar, available at https://yourstory.com/2016/11/vishal-dhupar-nvidia/, retrieved on December 12, 2017.

CENTRE FOR LAND WARFARE STUDIES (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Tel.: +91-11-25691308, Fax: +91-11-25692347, Email: landwarfare@gmail.com
Website: www.claws.in
CLAWS Army No. 33098