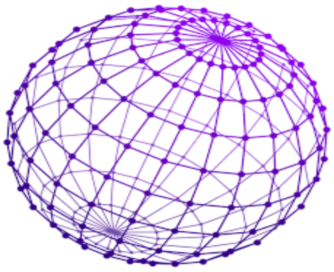
TECH WAVE

Technical Magazine

Department of Information Technology



HMR Institute of Technology & Management

(Affiliated with Guru Gobind Singh Indraprastha University)

Plot # 326, Hamidpur, Delhi-110036

Editorial Board – Tech Wave

Editor

D K Mishra

Assistant Professor – Department of Information Technology

Sub Editors

Adarsh Kumar 3rd Year B Tech (IT)

Simarn Pandey 3rd Year B Tech (IT)

Naman Jain 2nd Year B Tech (IT)

From Editor's Desk – Tech Wave

We, at HMRITM are delighted to announce the release of Tech Wave, A Technical Magazine, Department of Information Technology, HMR Institute of Technology & Management, Hamidpur, Delhi. The Tech Wave publishes technical articles which present novel research in the areas of engineering, science and technology.

We take this opportunity to thank all those contributors, reviewers, in making this magazine an unforgettable one. We would also like to thank our Chief Patron - Hon'ble Shri A K Gupta; Director General - Mr S N Jha (IAS – Retired); Director - Prof V C Pandey; Deputy Director - Prof Shalini Gupta; Head – Department of Information Technology, Dr Shafiqul Abidin; Head - Department of Computer Science & Engineering, Dr Mohd Izhar; Head - Department of Electronics & Communication Engineering, Dr Avadhesh Kumar Sharma, Head - Department of Electrical & Electronics Engineering, Dr U K Choudhary, Head - Department of Mechanical & Automation Engineering, Dr Ravindra Kumar, for their motivation and support in bringing out this edition of Tech Wave Magazine. Suggestions and feedback from our readers are welcome for the overall improvement of quality.

D K Mishra
Editor – Tech Wave
Assistant Professor – Department of Information Technology

Academic Year 2018-19

CONTENTS

Director's Message – HMRITM

I am happy that Department of Information Technology, HMRITM, Delhi, is bringing out a Institute Technical Magazine " Tech Wave". The Tech Wave will definitely help to show-case the activities that are happening in Department and the Campus. It also helps in building up teamwork which is very much needed today in the world of competition. It provides a platform for exposing the merits and academic achievements of the faculty and students. This enhances the documentation culture of the institute. This would definitely create an impact in the minds of readers, by way of providing larger visibility and dimension to the campus. I hope that this culture of releasing Technical Magazine continue forever and become a quoted example for all other colleges to follow.

Dr V C Pandey
Professor & Director – HMRITM

From HoD's Desk – Department of Information Technology

We are happy to inform that our pride rests in the Annual Technical Magazine ***'Tech Wave'***, which highlights the academic and non-academic activities of both staff and students of the department.

The field of Information Technology is ever changing and ever evolving branch. Innovation, orientation and an ever expanding base serve as a firm foundation for the latest development in the department of Information Technology. '***Tech Wave'*** would provide a platform for all HMRITIANS to interact with each other. We will share our achievements and happenings on the department campus. Magazine contains technical articles, faculty & student's achievements and many more.

The department is imparting the required technical and practical knowledge to the students. The department has substantial number of experienced faculty members. Every effort is made to constantly improve the results of the students. I am very happy to inform that due to the concerted efforts of staff, students and encouragement & support from the management, the results and placements are overwhelming.

We invite our readers to respond to the '***Tech Wave'*** immediately with suggestions, criticisms and scope of improvement so that this magazine takes a genuine interactive shape.

Dr Shafiqul Abidin
Professor & Head – Department of Information Technology

Vision & Missions, Programme Specific Outcomes & Programme Educational Objectives – Department of Information Technology

The department of IT started functioning in the academic year 2003. Since its inception the department is committed to meet its vision and missions.

Vision of the Department : Empowering through quality technical education and project based learning for producing socially responsible technocrats to meet the current and future requirements of IT industries.

Missions of the Department:

- Impart quality education through flexible and innovative teaching learning process to meet the needs of industries, business and society.
- Enable and ignite young minds to excel in their career and life with entrepreneurial spirit, professional ethics and human values.
- As a unified community of faculty, staff and students, we work together with the spirit of collaboration and partnership to accomplish our vision.
- Establish industry and academia collaborations to fill academic-industry gap.

Programme Specific Outcomes (PSOs) of the Department:

- Foundation of mathematical concepts: To use mathematical methodologies to work out problems using suitable mathematical analysis, data structure and suitable algorithms.
- Foundation of Information System: the ability to interpret the fundamental concepts and methodology of IT Systems. Students can understand the functionality of hardware and software aspects of computer systems.
- Foundations of Software Development: The ability to design , develop and test the software development projects. Familiarity and practical proficiency with a broad area of programming concepts and provide new ideas and innovations towards research.
- Information Communication System (ICT): Ability to apply concept of communication & wireless technology. Analyze & recommend the appropriate IT infrastructure required for the implementation of IT projects.

Program Educational Objectives (PEOs) of the Department:

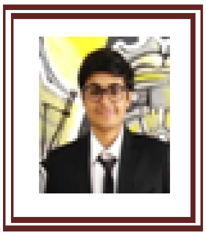
- Train to exhibit effective technical, communication and project management skills in their profession by following ethical practices.
- Excel in Professional career by acquiring knowledge in information technology and engineering principles.
- Graduate are capable of pursuing higher education and research.

Toppers of the Department

2015-19

Rachit Mann (86.05%)

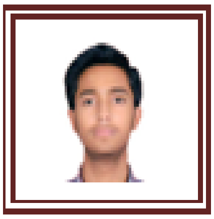
Atul Aman(82.99%)



Sarthak Sareen(80.3%)

2016-20

Kanika Gupta (85.8%)



Shubham K. Singh (83.7%)

Mohit Bhambri (83.6%)

2017-21

Hemlata (83.4%)

Simran Pandey (82.9%)

Rajat Bhardwaj (80.2%)

2018-22

Nitin Tyagi (86.8%)

Jaya Gupta (85.2%)

Nancy Mangla (82.4%)

Students' Project and Technical Exposure

The Information Technology (IT) Department regularly conducts Value Addition Programmes (VAP). VAP has been proved useful to fill the academic-industrial gap. All the departments of the Institute believe that Project Based Learning (PBL) is one of the key constituents to improve the overall quality of the students' projects. HMR Institute of Technology & Management conducts Tech-Expo – an annual technical project exhibition, a platform to show-case the practical and applicable model (project).

Thus by employing VAP, PBL and organizing Annual Tech – Expo, students have been showing their skills in their project works.

Few of the projects developed by IT students are listed below:

Marketing and Sales Analysis by Vipluv Mittal

Sentiment Analysis by Vasvi Batra, Aabhas Jain and Anuj Khanna

Traffic Sign Recognition by Trishala Bhasin, Aditi Kanodia and Meghna Goel

DIP for Automatic Surveillance and IS by Sahil Sharma and Sneh Rathore

Photo OCR using ML Algorithms by Aditya Malik

The Silver Screen Game by Srishti Sachdeva and Prakul Manik

Android Based Custom ROM by Abhishek Gupta, Rohit Gupta, Himanshu Prajapati and Kapil Tripathi

Remote Desktop Application by Sunil, Shailender Singh, Sanchali, Rajeev and Joy

Android Control Spy Robot by Yatharth Gupta, Aman Gupta, Krishna and Divyansh (EEE).

One of the Projects entitled " **Computer Forensics and Security using Python**", developed by **HEMANT KUMAR** bagged **FIRST PRIZE** in Guru Gobind Singh Indraprastha University, Inter-College B Tech Major Project Competition, organized by University School of Information, Communication and Technology, GGSIPU, New Delhi.

One of the Projects entitled " **Computer Forensics and Security using Python**", developed by **HEMANT KUMAR** bagged **FIRST PRIZE** in Guru Gobind Singh Indraprastha University, Inter-College B Tech Major Project Competition, organized by University School of Information, Communication and Technology, GGSIPU, New Delhi.

Tech Expo – An Annual Technical Project Exhibition was held in April 2019, in this event around 70 students of IT department participated. These projects were judged and assessed by external experts from academics and industries. The following students bagged the prizes.

Project Name	**Students Participated**	**Position**
Intrusion Security System	Shakti Singh	First Position *
	S.Vishnu Vardhan Reddy	
	Aajay Kumar Sharma	
UML Tool	Chaitanya Sanoriya	First Position*
	Rachit Mann	
	Sarthak Sareen	
	Arun Kumar	
Bus Management System	Harshul Gupta	Second Position
	Tushar Garg	
	Yash Bhardwaj	

* These projects secured same marks and therefore both teams declared Winners.

HCL Visit

For technical exposure students of the department visit industries regularly. HCL Noida invited our students to have an idea about recent technologies and future job prospects.

Students enjoyed HCL visit and found themselves technically enhanced.

Benefits & Risks of Artificial Intelligence

Adarsh Kumar

B Tech Scholar
Department of IT, HMR Institute of Technology & Management, (GGSIPU), Delhi, India
ak6432890@gmail.com

Everything we love about civilization is a product of intelligence, so amplifying our human intelligence with artificial intelligence has the potential of helping civilization flourish like never before – as long as we manage to keep the technology beneficial.“

Max Tegmark, President of the Future of Life Institute

1 Introduction

From SIRI to self-driving cars, artificial intelligence (AI) is progressing rapidly. While science fiction often portrays AI as robots with human-like characteristics, AI can encompass anything from Google's search algorithms to IBM's Watson to autonomous weapons.

Artificial intelligence today is properly known as narrow AI (or weak AI), in that it is designed to perform a narrow task (e.g. only facial recognition or only internet searches or only driving a car). However, the long-term goal of many researchers is to create general AI (AGI or strong AI). While narrow AI may outperform humans at whatever its specific task is, like playing chess or solving equations, AGI would outperform humans at nearly every cognitive task.

2 Why Research AI Safety?

In the near term, the goal of keeping AI's impact on society beneficial motivates research in many areas, from economics and law to technical topics such as verification, validity, security and control. Whereas it may be little more than a minor nuisance if your laptop crashes or gets hacked, it becomes all the more important that an AI system does what you want it to do if it controls your car, your airplane, your pacemaker, your automated trading system or your power grid. Another short-term challenge is preventing a devastating arms race in lethal autonomous weapons.

In the long term, an important question is what will happen if the quest for strong AI succeeds and an AI system becomes better than humans at all cognitive tasks. As pointed out by I.J. Good in 1965, designing smarter AI systems is itself a cognitive task. Such a system could potentially undergo recursive self-improvement, triggering an intelligence explosion leaving human intellect far behind. By inventing revolutionary new technologies, such a super intelligence might help us eradicate war, disease, and poverty, and so the creation of strong AI might be the biggest event in human history. Some experts have expressed concern, though, that it might also be the last, unless we learn to align the goals of the AI with ours before it becomes super intelligent.

There are some who question whether strong AI will ever be achieved, and others who insist that the creation of super intelligent AI is guaranteed to be beneficial. At FLI we recognize both of these possibilities, but also recognize the potential for an artificial intelligence system to intentionally or unintentionally cause great harm. We believe research today will help us better prepare for and prevent such potentially negative consequences in the future, thus enjoying the benefits of AI while avoiding pitfalls.

3 How can AI be dangerous?

Most researchers agree that a super intelligent AI is unlikely to exhibit human emotions like love or hate, and that there is no reason to expect AI to become intentionally benevolent or malevolent. Instead, when considering how AI might become a risk, experts think two scenarios most likely:

The AI is programmed to do something devastating: Autonomous weapons are artificial intelligence systems that are programmed to kill. In the hands of the wrong person, these weapons could easily cause mass casualties. Moreover, an AI arms race could inadvertently lead to an AI war that also results in mass casualties. To avoid being thwarted by the enemy, these weapons would be designed to be extremely difficult to simply “turn off,” so humans could plausibly lose control of such a situation. This risk is one that’s present even with narrow AI, but grows as levels of AI intelligence and autonomy increase.

The AI is programmed to do something beneficial, but it develops a destructive method for achieving its goal: This can happen whenever we fail to fully align the AI’s goals with ours, which is strikingly difficult. If you ask an obedient intelligent car to take you to the airport as fast as possible, it might get you there chased by helicopters and covered in vomit, doing not what you wanted but literally what you asked for. If a super intelligent system is tasked with a ambitious geo engineering project, it might wreak havoc with our ecosystem as a side effect, and view human attempts to stop it as a threat to be met.

As these examples illustrate, the concern about advanced AI isn’t malevolence but competence. A super-intelligent AI will be extremely good at accomplishing its goals, and if those goals aren’t aligned with ours, we have a problem. You’re probably not an evil ant-hater who steps on ants out of malice, but if you’re in charge of a hydroelectric green energy project and there’s an anthill in the region to be flooded, too bad for the ants. A key goal of AI safety research is to never place humanity in the position of those ants.

4 Why the recent interest in AI safety

Stephen Hawking, Elon Musk, Steve Wozniak, Bill Gates, and many other big names in science and technology have recently expressed concern in the media and via open letters about the risks posed by AI, joined by many leading AI researchers. Why is the subject suddenly in the headlines?

The idea that the quest for strong AI would ultimately succeed was long thought of as science fiction, centuries or more away. However, thanks to recent breakthroughs, many AI milestones, which experts viewed as decades away merely five years ago, have now been reached, making many experts take seriously the possibility of super intelligence in our lifetime. While some experts still guess that human-level AI is centuries away, most AI researches at the 2015 Puerto Rico Conference guessed that it would happen before 2060. Since it may take decades to complete the required safety research, it is prudent to start it now.

Because AI has the potential to become more intelligent than any human, we have no surefire way of predicting how it will behave. We can’t use past technological developments as much of a basis because we’ve never created anything that has the ability to, wittingly or unwittingly, outsmart us. The best example of what we could face may be our own evolution. People now control the planet, not because we’re the strongest, fastest or biggest, but because we’re the smartest. If we’re no longer the smartest, are we assured to remain in control?

FLI’s position is that our civilization will flourish as long as we win the race between the growing power of technology and the wisdom with which we manage it. In the case of AI technology, FLI’s position is that the best way to win that race is not to impede the former, but to accelerate the latter, by supporting AI safety research.

5 The future is now: AI’s impact is everywhere

There’s virtually no major industry modern AI — more specifically, “narrow AI,” which performs objective functions using data-trained models and often falls into the categories of deep learning or machine learning — hasn’t already affected. That’s especially true in the past few years, as data collection and analysis has ramped up considerably thanks to robust IoT connectivity, the proliferation of connected devices and ever-speedier computer processing.

Some sectors are at the start of their AI journey, others are veteran travelers. Both have a long way to go. Regardless, the impact artificial intelligence is having on our present day lives is hard to ignore:

- Transportation: Although it could take a decade or more to perfect them, autonomous cars will one day ferry us from place to place.
- Manufacturing: AI powered robots work alongside humans to perform a limited range of tasks like assembly and stacking, and predictive analysis sensors keep equipment running smoothly.
- Health care: In the comparatively AI-nascent field of health care, diseases are more quickly and accurately diagnosed, drug discovery is sped up and streamlined, virtual nursing assistants monitor patients and big data analysis helps to create a more personalized patient experience.

- Education: Textbooks are digitized with the help of AI, early-stage virtual tutors assist human instructors and facial analysis gauges the emotions of students to help determine who’s struggling or bored and better tailor the experience to their individual needs.

- Media: Journalism is harnessing AI, too, and will continue to benefit from it. Bloomberg uses Cyborg technology to help make quick sense of complex financial reports. The Associated Press employs the natural language abilities of Automated Insights to produce 3,700 earning reports stories per year — nearly four times more than in the recent past.

- Customer Service: Last but hardly least, Google is working on an AI assistant that can place human-like calls to make appointments at, say, your neighborhood hair salon. In addition to words, the system understands context and nuance.

Importance of Machine Learning

Simran Pandey

B Tech Scholar
Department of IT, HMR Institute of Technology & Management, (GGSIPU), Delhi, India
simranpandey16@gmail.com

Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

1 Introduction

Machine learning is nothing new. The history, in fact, dates back over sixty years to when Alan Turing created the ‘Turing test’ to determine whether a computer had real intelligence. It can be argued, however, that the past 25-30 years have seen the biggest leaps and bounds in terms of advances in speech technology. But I’m getting ahead of myself here.

While artificial intelligence (AI) is the broad science of mimicking human abilities, machine learning is a specific subset of AI that trains a machine how to learn. Watch this video to better understand the relationship between AI and machine learning. You'll see how these two technologies work, with useful examples and a few funny asides.

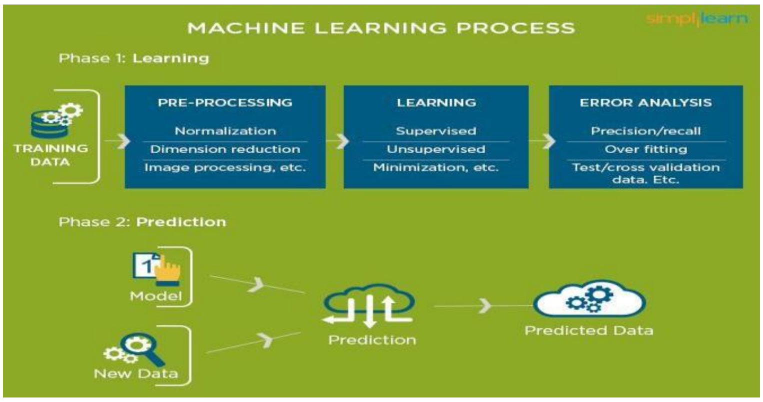


Fig. 1. Process of Machine Learning.

2 Evolution of Machine Learning

Because of new computing technologies, machine learning today is not like machine learning of the past. It was born from pattern recognition and the theory that computers can learn without being programmed to perform specific tasks; researchers interested in artificial intelligence wanted to see if computers could learn from data. The iterative aspect of machine learning is important because as models are exposed to new data, they are able to independently adapt. They learn from previous computations to produce reliable, repeatable decisions and results. It’s a science that’s not new – but one that has gained fresh momentum.

- While many machine learning algorithms have been around for a long time, the ability to automatically apply complex mathematical calculations to big data – over and over, faster and faster – is a recent development. Here are a few widely publicized examples of machine learning applications you may be familiar with:
- The heavily hyped, self-driving Google car? The essence of machine learning.
- Online recommendation offers such as those from Amazon and Netflix? Machine learning applications for everyday life.
- Knowing what customers are saying about you on Twitter? Machine learning combined with linguistic rule creation.
- Fraud detection? One of the more obvious, important uses in our world today.

3 Exploring Data Mining, Machine Learning and Deep Learning

While all three disciplines listed above are in the same family, it's essential to understand how they differ. At a basic level, Machine Learning uses the same algorithms and techniques like data mining, but the types of predictions the two provide vary. Data mining discovers previously unknown patterns and knowledge, whereas Machine Learning reproduces known patterns and knowledge. ML then automatically applies that information to additional datasets, and, ultimately, the business strategy and outcomes.

Deep learning, on the other hand, uses advanced computing power and special types of neural networks and applies them to large amounts of data to learn, understand, and identify complicated patterns. Automatic language translation and medical diagnoses are examples of deep learning.

4 Popular Machine Learning Methods

How do machines learn? Two Machine Learning techniques are supervised learning and unsupervised learning. Approximately 70 percent of Machine Learning is supervised learning, while unsupervised learning ranges from 10 – 20 percent. Other methods that are used less often include semi-supervised and reinforcement learning.

4.1 Supervised Learning

This kind of learning is possible when inputs and outputs are identified, and algorithms are trained using labeled examples. To understand this better, let's consider the following example: a piece of equipment could have data points labeled F (failed) or R (runs).

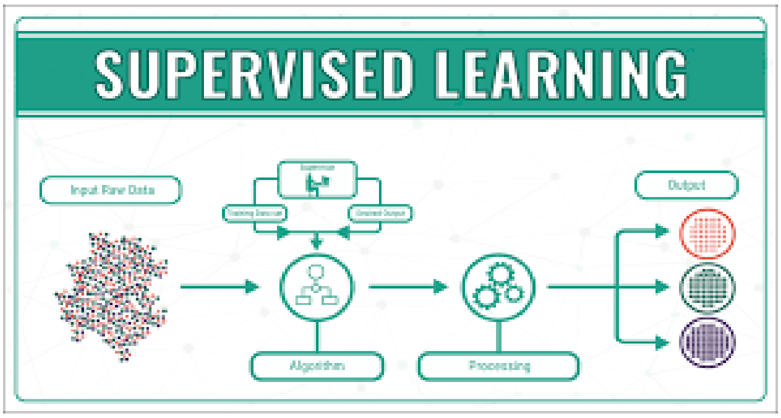


Fig. 2. Supervised Learning.

The supervised learning algorithm receives a set of inputs along with the corresponding output to find errors. Based on these inputs, it would modify the model accordingly. This is a form of pattern recognition since supervised learning uses methods like classification, regression, prediction, and gradient boosting. Supervised learning then uses these patterns to predict the values of the label on other unlabeled data.

Supervised learning is typically used in applications with which historical data predicts future events, such as fraudulent credit card transactions.

4.2 Unsupervised Learning

Unlike supervised learning, unsupervised learning works with data sets without historical data. An unsupervised learning algorithm explores collected data to find a structure. This works best for transactional data; for instance, it helps identify customer segments and clusters with specific attributes, often used in content personalization.

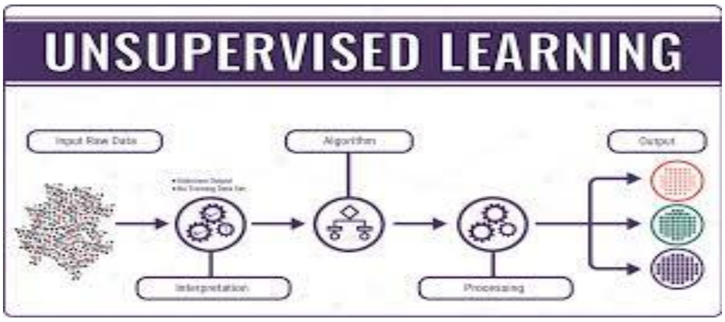


Fig. 3. Unsupervised Learning.

Popular techniques where unsupervised learning is used also include self-organizing maps, nearest-neighbor mapping, singular value decomposition, and k-means clustering. In other words: online recommendations, identification of data outliers, and segment text topics are examples of unsupervised learning.

4.3 Semi-Supervised Learning

As the name suggests, semi-supervised learning is a bit of both supervised and unsupervised learning and uses both labeled and unlabeled data for training. In a typical scenario, the algorithm uses a small amount of labeled data with a large amount of unlabeled data.

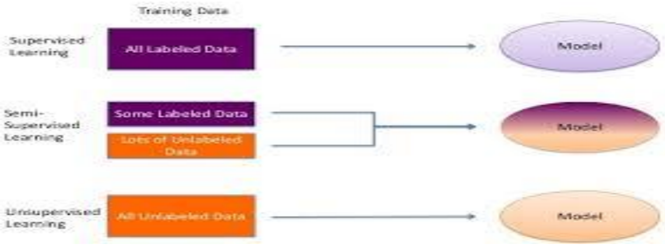


Fig. 4. Semi-Supervised Learning.

We use this type of Machine Learning for classification, regression, and prediction. Examples of semi-supervised learning are face- and voice-recognition applications.

4.4 Reinforcement Learning

Reinforcement learning occurs when the agent chooses actions that maximize the expected reward over a given time. This is easiest to achieve when the agent is working within a sound policy framework.

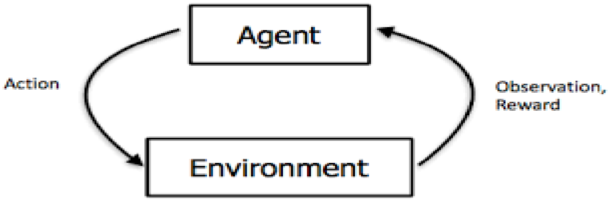


Fig. 5. Reinforcement Learning.

4.5 Practical Applications

Machine learning has several very practical applications that drive the kind of real business results – such as time and money savings – that have the potential to dramatically impact the future of your organization. At Interactions in particular, we see tremendous impact occurring within the customer care industry, whereby machine learning is allowing people to get things done more quickly and efficiently. Through Virtual Assistant solutions, machine learning automates tasks that would otherwise need to be performed by a live agent – such as changing a password or checking an account balance. This frees up valuable agent time that can be used to focus on the kind of customer care that humans perform best: high touch, complicated decision-making that is not as easily handled by a machine. At Interactions, we further improve the process by eliminating the decision of whether a request should be sent to a human or a machine: unique Adaptive Understanding technology, the machine learns to be aware of its limitations, and bail out to humans when it has a low confidence in providing the correct solution.

Machine learning has made dramatic improvements in the past few years, but we are still very far from reaching human performance. Many times, the machine needs the assistance of human to complete its task. At Interactions, we have deployed Virtual Assistant solutions that seamlessly blend artificial with true human intelligence to deliver the highest level of accuracy and understanding.

5 Research Areas and AI Safety

Humanity‘s social and technological dominance stems primarily from our proficiency at reasoning, planning, and doing science (Armstrong). We will call this capacity general intelligence (Muehlhauser) general‖ because humans didn‘t need to evolve separate modules for doing theoretical physics, software engineering, and heart surgery over millions of years. Instead, a relatively small set of adaptations separating humans from chimpanzees must simultaneously enable all of these capabilities.

It is this general problem-solving ability that we have in mind when we talk about ―artificial general intelligence‖ (AGI) or smarter-than-human AI.‖ AI systems may come to surpass humans in science and engineering abilities without being particularly human-like in any other respects — artificial intelligence need not imply artificial consciousness, for example, or artificial emotions. Instead, we have in mind the capacity to model real-world environments well and identify a variety of ways to put those environments into new states. The case for focusing on AI risk mitigation doesn‘t assume much about how future AI systems will be implemented or used. Here are the claims that we think of as key:

- Whatever problems/tasks/objectives we assign to advanced AI systems probably won‘t exactly match our real-world objectives. Unless we put in an (enormous, multi-generational) effort to teach AI systems every detail of our collective values (to the extent there is overlap), realistic systems will need to rely on imperfect approximations and proxies for what we want (Soares, Yudkowsky).
- If the system‘s assigned problems/tasks/objectives don‘t fully capture our real objectives, it will likely end up with incentives that catastrophically conflict with what we actually want (Bostrom, Russell, Benson-Tilsen & Soares).
- AI systems can become much more intelligent than humans (Bostrom), to a degree that would likely give AI systems a decisive advantage in arbitrary conflicts (Soares, Branwen).
- It‘s hard to predict when smarter-than-human AI will be developed: it could be 15 years away, or 150 years (Open Philanthropy Project). Additionally, progress is likely to accelerate as AI approaches human capability levels, giving us little time to shift research directions once the finish line is in sight (Bensing)

6 Limitations and Drawbacks

Artificial Intelligence (AI) is poised to disrupt our world. With intelligent machines enabling high-level cognitive processes like thinking, perceiving, learning, problem-solving and decision making, coupled with advances in data collection and aggregation, analytics and computer processing power, AI presents opportunities to complement and supplement human intelligence and enrich the way people live and work.

On the other hand, some of the leading scientists and thinkers have warned about 'technological singularity'. Technological singularity refers to the belief that ordinary humans will someday be overtaken by artificially intelligent machines or cognitively enhanced biological intelligence, or both.

It is a technology that takes in huge amounts of information from a specific domain and uses it to make a decision in the service of a specified goal. For example, AI technology can be used to analyze loan repayment histories (information) of a person to decide whether to give an individual a loan or not (decision) so as to maximize the profits for the lender (goal). In 2016, Google-run artificial intelligence (AI) programme "AlphaGo" defeated legendary player Lee Se-dol in Go - a complex Chinese board game that is considered the "quintessential unsolved problem" for machine intelligence. Though the AI has many benefits, it has sparked up a debate about its dangers to humanity.AI machines are like other human beings in terms of their capacities for decision and action. They cannot be compared to other machines as the degree of independence that AI technologies have is much more complex. AI is an attempt to reproduce super intelligent humans. It chooses one aspect of human beings, namely the intelligence, and artificially magnifies it to an extent that allows the machine to do things far better than humans can.

AI is associated with superlative memory, calculative power, decision-making capacity, high speeds of action, etc. These machines thus become super-beings, and a society filled with many super-beings is a recipe for disaster. AI machines are a mirror to our desire for immortality and the absence of human weaknesses.Most importantly, the AI has not been used to get rid of poverty, to have a more equitable distribution of wealth, or to make people more content with what they have. Instead, they will primarily be dictated by profit for the companies that make them.

7 AI and Recent Development

Artificial Intelligence (AI) is one of the major developments of our time. Machine learning, and the implications that go with it, are shaking up many aspects of how we do things, allowing us to deploy AI where we previously used a human or a more inefficient process. Sometimes this is to the consternation of people, particularly those who worry about AI taking human jobs, or perhaps the sci-fi scenario of AI being intelligent and organized enough to overrule humans. One thing we do know is that we‗ve probably only scratched the surface in terms of what is possible. As Oracle EVP and head of applications, Steve Miranda said at a recent event, ―Two years from now, we‗ll probably be talking about a whole new set of things in this category that probably none of us is even thinking about today.‖ Well, that‗s an exciting thought, considering how far we‗ve already come! Here are some recent developments in AI, which demonstrate how the technology is advancing:

- Automatic Machine Learning Will Be The Next High Point : ―Reinforcement Learning‖.
- The Dawn Of Quantum Computing With AI.
- Social Economic Models.
- A Digital Drift Of Neural Networks.
- Facial Recognization: An Innovation.
- Biased Data..
- Privacy And Policy

Deep Learning – An Emerging Paradigm

Vinay Bansal

B Tech Scholar
Department of IT, HMR Institute of Technology & Management, (GGSIPU), Delhi, India
bina.bansal@gmail.com

The lowdown on deep learning: from how it relates to the wider field of machine learning through to how to get started with it.

1 Definition – Deep Learning

Deep learning is a subset of machine learning, which itself falls within the field of artificial intelligence.

2 Comparisons among Deep Learning, Machine Learning and Artificial Intelligence

Artificial intelligence is the study of how to build machines capable of carrying out tasks that would typically require human intelligence.That rather loose definition means that AI encompasses many fields of research, from genetic algorithms to expert systems, and provides scope for arguments over what constitutes AI.Within the field of AI research, machine learning has enjoyed remarkable success in recent years -- allowing computers to surpass or come close to matching human performance in areas ranging from facial recognition to speech and language recognition.

Machine learning is the process of teaching a computer to carry out a task, rather than programming it how to carry that task out step by step.At the end of training, a machine-learning system will be able to make accurate predictions when given data.That may sound dry, but those predictions could be answering whether a piece of fruit in a photo is a banana or an apple, if a person is crossing in front of a self-driving car, whether the use of the word book in a sentence relates to a paperback or a hotel reservation, whether an email is spam, or recognizing speech accurately enough to generate captions for a YouTube video.Machine learning is typically split into supervised learning, where the computer learns by example from labeled data, and unsupervised learning, where the computer groups similar data and pinpoints anomalies.

Deep learning is a subset of machine learning, whose capabilities differ in several key respects from traditional shallow machine learning, allowing computers to solve a host of complex problems that couldn't otherwise be tackled.An example of a simple, shallow machine-learning task might be predicting how ice-cream sales will vary based on outdoor temperature. Making predictions using only a couple of data features in this way is relatively straightforward, and can be carried out using a shallow machine-learning technique called linear regression with gradient descent.The issue is that swathes of problems in the real world aren't a good fit for such simple models. An example of one of these complex real-world problems is recognizing handwritten numbers.

To solve this problem, the computer needs to be able to cope with huge variety in how the data can be presented. Every digit between 0 and 9 can be written in myriad ways: the size and exact shape of each handwritten digit can be very different depending on who's writing and in what circumstance.Coping with the variability of these features, and the even bigger mess of interactions between them, is where deep learning and deep neural networks become useful.Neural networks are mathematical models whose structure is loosely inspired by that of the brain.Each neuron within a neural network is a mathematical function that takes in data via an input, transforms that data into a more amenable form, and then spits it out via an output. You can think of neurons in a neural network as being arranged in layers, as shown in figure.

All neural networks have an input layer, where the initial data is fed in, and an output layer, that generates the final prediction. But in a deep neural network, there will be multiple "hidden layers" of neurons between these input and output layers, each feeding data into each other. Hence the term "deep" in "deep learning" and "deep neural networks", it is a reference to the large number of hidden layers -- typically greater than three -- at the heart of these neural networks.

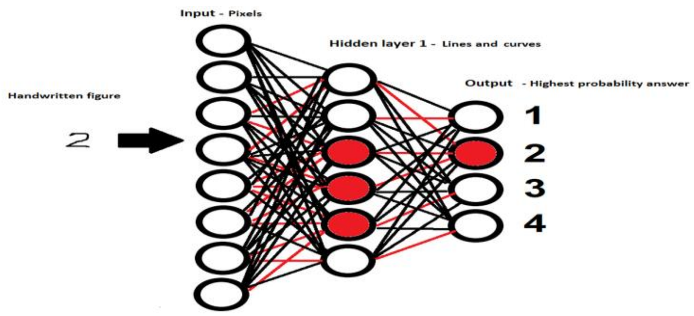

Input - Pixels
Hidden layer 1 - Lines and curves
Output - Highest probability answer
Handwritten figure
2
1
2
3
4

Fig. 2. Depiction of Process.

This simplified diagram above hopefully helps to provide an idea of how a simple neural network is structured. In this example, the network has been trained to recognize handwritten figures, such as the number 2 shown here, with the input layer being fed values representing the pixels that make up an image of a handwritten digit, and the output layer predicting which handwritten number was shown in the image.In the diagram above, each circle represents a neuron in the network, with the neurons organized into vertical layers.

3 Why is it called Deep Learning?

As mentioned, the depth refers to the number of hidden layers, typically more than three, used within deep-neural networks.

3.1 How is Deep Learning being used?

For many tasks, for recognizing and generating images, speech and language, and in combination with reinforcement learning to match human-level performance in games ranging from the ancient, such as Go, to the modern, such as Dota 2 and Quake III.Deep-learning systems are a foundation of modern online services. Such systems are used by Amazon to understand what you say -- both your speech and the language you use -- to the Alexa virtual assistant or by Google to translate text when you visit a foreign-language website.Every Google search uses multiple machine-learning systems, to understand the language in your query through to personalizing your results, so fishing enthusiasts searching for "bass" aren't inundated with results about guitars.But beyond these very visible manifestations of machine and deep learning, such systems are starting to find a use in just about every industry. These uses include: computer vision for driver less cars, drones and delivery robots; speech and language recognition and synthesis for chat bots and service robots; facial recognition for surveillance in countries like China; helping radiologists to pick out tumors in x-rays, aiding researchers in spotting genetic sequences related to diseases and identifying molecules that could lead to more effective drugs in health care; allowing for predictive maintenance on infrastructure by analyzing IoT sensor data; underpinning the computer vision that makes the cashier less Amazon Go supermarket possible, offering reasonably accurate transcription and translation of speech for business meetings -- the list goes on and on.

4 How to use Deep Learning?

When your data is largely unstructured and you have a lot of it.Deep learning algorithms can take messy and broadly unlabeled data -- such as video, images, audio recordings, and text -- and impose enough order upon that data to make useful predictions, building a hierarchy of features that make up a dog or cat in an image or of sounds that form a word in speech.

- IoT boom will change how data is analysed
- Sorry, general AI is still a long, long way off
- These 10 technologies are most likely to help save planet Earth
- Google's war on deepfakes: As election looms, it shares ton of AI-faked videos

5 Deep Learning Software

There are a wide range of deep-learning software frameworks, which allow users to design, train and validate deep neural networks, using a range of different programming languages.A popular choice is Google's TensorFlow software library, which allows users to write in Python, Java, C++, and Swift, and that can be used for a wide range of deep learning tasks such as image and speech recognition, and which executes on a wide range of CPUs, GPUs, and other processors. It is well-documented, and has many tutorials and implemented models that are available.Another popular choice, especially for beginners, is PyTorch, a framework that offers the imperative programming model familiar to developers and allows developers to use standard Python statements. It works with deep neural networks ranging from CNNs to RNNs and runs efficiently on GPUs.Among the wide range of other options are Microsoft's Cognitive Toolkit , MATLAB, MXNet, Chainer, and Keras.

5 Neural Network and Deep Learning

At present deep learning is used to build narrow AI, artificial intelligence that performs a particular task, be that captioning photos or transcribing speech.There's no system so far that can be thought of as a general artificial intelligence, able to tackle the same breadth of tasks and with the same broad understanding as a human being. When such systems will be developed is unknown, with predictions ranging from decades upwards.

On Confidentiality, Integrity, Authenticity and Freshness (CIAF) in WSN

D K Misra[1] , Anupam Sharma[2], Atul Kumar [3]

[1,2,3] HMR Institute of Technology & Management, (GGSIPU), Delhi, India
[1] misra.deven@gmail.com, [2]anupamsharma243@gmail.com, [3]atul.mtech.it@gmail.com

Abstract. A Wireless Sensor Network (WSN) comprises several sensor nodes such as magnetic, thermal, and infrared and the radar is setup in a particular geographical area. The primary aim of Sensor Network is to transmit reliable, secure data from one node to another node, node to base station and vice versa and from base station to all nodes in a network and to conserve the energy of sensor nodes. On the other hand, there are several restrictions such as large energy consumption, limited storage/memory and processing ability, higher latency and insufficient resources. The related security issues in Wireless Sensor Network are Authenticity, confidentiality, Robustness, Integrity and Data Freshness. The sensor nodes are susceptible to several attacks such as DOS, Sybil, Flood, Black hole, Selective Forwarding which results in the leakage of sensitive and valuable information. It is therefore necessary to provide security against these critical attacks in the network. Wireless Sensor Network were earlier used for military applications with the objective of monitoring friendly and opposing forces, battlefield surveillance, detection of attacks, but today Wireless Networking have a huge number of applications-environmental, healthcare, home, industrial, commercial and are still counting. This paper in an extensive review of the security requirements, attacks that are to be avoided and resolved for achieving a secure network connection. This paper also emphasizes various limitations and defense strategies to prevent threats & attacks. The issues of applications of Wireless Sensor Network for smooth and reliable transmissions are also discussed. The sensor networks are popular for mission-critical-tasks and security is immensely required for such hostile environment employed networks.

Keywords: Cryptography; Data Confidentiality; Sybil; Data Authentication; Blackhole Attack; Attacks on WSN.

1 Introduction

During the past years, Wireless Sensor Network has found a huge number of applications in various fields that can have a significant impact on the society. Sensor network may consist of many different types of sensor nodes such as magnetic, thermal, infrared and radar which are able to monitor a wide number of environmental conditions, possessing either unique or different features, designated with some pre-determined functions and functionalities. A sensor network consists of a large number of tiny sensor nodes and their number in a network may range from few, to hundreds, to thousands even more and possibly a few powerful nodes called base stations. These nodes are capable of communicating with each other by means of single or multiple channels. Multiple channel-based communications are preferred over single channel due to reliable communication, less collisions or interferences, greater bandwidth and improved network throughput. Base stations are responsible for aggregating the data, monitoring and network management [1]. Base stations act as a gateway between the sensor nodes and the base stations. The WSN also includes task manager, network manager, security manager communication hardware and compatible software as its related components. The principle working mechanism of WSN is that the sensor nodes senses, accumulates data from varied locations in the environment, co-operates among themselves, processes the information and then transmits the data to the main location that is base station. Some important parameters need to be considered while designing a network: end-to-end latency [2] (should decrease), energy consumption (should be less), packet delivery ratio (should be high), and throughput (should increase). These factors play a significant role in determining the efficiency of the network. Routing in another fundamental aspect of sensor network, determining the path between source and destination, and leads to secure transmission of data packets and can also help optimize application availability, improves productivity and responsiveness. The need for secure transmission resulted in the development of different routing protocols and algorithms [3]. The routing protocols are categorized in four broad categories-based on network structure, based on protocol operation, based on path establishment, and based on the initiator of communication.

The wireless sensor networks are considered application-specific. There are huge applications of wireless sensor networks including sensor based alarming / fire system, smart homes and farming/harvesting, structural health monitoring, habitat monitoring, civil engineering, surveillance and emergency response systems, environmental research, disaster management, robotics, traffic monitoring, transportation and logistics, military, tracking, industrial and consumer process, monitoring and control applications [4]. The wide range of applications of the sensor network requires each sensor to be highly diminished in terms of size, power consumption and price.

One of the primary concerns of WSN is that transmitted information should be safe and secure [5]. No one should be allowed to access network and information. It is possible that a third party after receiving data packets may create mess and nuisance with the original packets if there is no secure mechanism has been implemented or imposed to protect data between nodes. To implement this, it is mandatory to explore challenges in design, intelligent applications with minimum memory and shortage of computing power. Further, tough radio transmission bandwidth is also needed. In short, smart security mechanisms are required to protect, detect and pull through severe attacks. Levels of implementing these mechanisms may differ according to the nature of attacks. The transmitted data need to be confidential, authentic, private, robust, and sustainable and should also maintain the forward and backward secrecy [6]. WSN security is somewhat different from local area networks and wide area networks because sensor nodes equipped with computer power, battery, wireless, ad hoc, Unattended. Therefore, due to these limitations as well as constraints in WSNs a large number of protocols are rely on Symmetric Key Cryptography. Key management (use of global, pair wise and symmetric keys), encryption, secure data aggregations are some of the commonly employed security solutions for wireless sensor networks. There are different techniques that are used to prolong the lifetime of a sensor network [7]. The security requirements for WSN are: - Confidentiality, Integrity, Availability, and Freshness [20].

Additional requirements may include Authentication, Access Control, Privacy, Authorization, Non-Repudiation and Survivability.

The paper has been narrated in the following manner: Section 2 highlights constraints and limitations, whereas section 3 emphasizes upon the concerned security issues, requirements and the need of providing security in wireless sensor networks, section 4 discusses the attacks/threats on WSN and also the defensive measures required to counter those attacks, section 5 finally provides the conclusion, which briefly summarizes the paper.

2 Constraints in Wireless Sensor Network

In this section limitations and constraints on WSN have been discussed that are differentiated from a large number of interconnected sensor nodes and the sensor field. WSN is non-resistant to attacks where an adversary may alter original data, inject corrupt data, capture data, floods a particular node with same message repeatedly and perform other such restricted activities, which often results in data loss, misrouting, delays, destroy the network resources and the nodes are at a risk of physically being damaged. Malicious node can be added to exhaust other sensor node capability affecting the whole environment. Large energy consumption, limited storage/memory and processing ability, higher latency, lesser reliability, scalability and fault-tolerance, risky operating environment, poor data aggregation [8], slow data processing speed and its optimization, computation and communication capabilities are some of the constraints in the network.

Energy is a very important factor in a WSN. Energy determines the life of a node. It is the most important criteria which distinguishes a normal node from an attacker node. Therefore, based on the different energy levels, attackers, cluster heads and base station are selected. There is energy loss when a packet is being sent or received. The reasons for energy loss in wireless sensor network communication [9]:

2.1 Control Packet Overhead

Control packet exhausts more energy in comparison with ordinary packets while transmission, receiving and listening, thereby it is useful to use less numbers of control packet for transmission, thus it reduces the overhead.

2.2 Collision

Basically, collision permits two or more stations try to exchange and transmit the data concurrently. When two stations transmit data concurrently, collision may likely to occur and the packets are junked and retransmitted and thereby resulting in energy loss.

2.3 Idle Listening

Idle listening refers to, when sensor listen for incoming packet even when no data is being sent. This results in energy loss of the node and depleting the lifetime of Wireless Sensor Network.

2.4 Overhearing

Overhearing: It is an indirect communication method where an agent receives packet which is not an addressee which results in unnecessary traffic which in turn results in energy loss.

Max-life (Maximum Lifetime) routing to balance the rate of energy consumption in different sensor nodes according to varying characteristics, EEMR (Energy Efficient Routing Algorithm) to improve the energy utilization by varying the activities of wireless communication modules of sensor network are some of the methodologies implemented for energy concerned issues [10].

3 Concerned Security Issues

It is very important to know and understand the security issues in WSN, prior to the knowledge of attacking techniques and the ways to prevent different attacks, so that the counter attack strategies may be developed more efficiently. Typical WSN consists of many nodes which have been assigned a particular energy level and malfunction of any node can cause damage to the whole working environment thereby decreasing the lifespan of that network. Some of the basic security issues in WSN are confidentiality, integrity, authenticity, which have been discussed below: -

3.1 Data Authentication

Authenticity is a process by which one verifies that someone is who they claim they are and not someone else. Authentication is to check the authenticity. In WSN authentication is a process by which the node makes sure that weather the incoming data is from correct source or has been injected by any intruder or any unknown surrounding network [11]. Data authentication puts on ice the acceptor that the data packet has not been altered during transmission. Authentication also makes sure that the data packets have been transmitted from exact source. Node Authenticity tells user about genuineness of individuality of sender node. If authentication is not present intruder without any obstacle can inject wrong data in the environment. Generally, to remove this problem of data authenticity Public Key Cryptography is used. Public key or asymmetric cryptography assigns same key to all the nodes in a particular network, so whenever a data is to be transmitted the sender node will only transmit the data if the receiving node has that public key and thus it verifies the authenticity of the node.

3.2 Data Confidentiality

Confidentiality means making something confidential. Sensor node transmit hypersensitive information. If an attacker node views data between the two nodes the confidentiality between the two nodes is broken. So, it is very important to keep in mind that any intruder cannot have access to hypersensitive data by intercepting the transmission between the two particular nodes. The most basic approach to attain data confidentiality is to provide a particular key and this process of assigning a particular key is called encryption. The data is assigned a particular key, encrypted with that key then it is transmitted and again decrypted at the receiving node with the help of that key, so even if the attacker views the data it cannot process it as that node does not have that particular key [12].

3.3 Robustness and Sustainability

If a node is attacked by an attacker node and the attacker node replaces the normal node, the working of the whole environment will be affected as now the attacker node will be having the particulars of a particular node in that environment. The sensor network should be robust against several intruder attacks, even if an intruder attack succeeds its encounter should be knocked down or decreased. System should be constructed so that it can tolerate and adapt to failure of a particular node. Each particular node should be designed to be as robust as possible.

3.4 Data Integrity

Integrity should be attained to verify that any intruder or unknown node cannot alter or modify the transmitted data. Data integrity ensures that the data being transmitted has not been altered during the transmission time and reaches the acceptor node in its original form. Data authentication may also be related to data integrity as data authentication provides data integrity.

3.5 Data Freshness

Data freshness signifies that no old data should be transmitted between the nodes which have already transmitted the same message i.e. data should be fresh. Each node in WSN are assigned with a particular energy level. Energy is spent whenever a node sends, accepts or process a data. In a particular wireless sensor network there is a possibility that an intruder or an attacker can catch hold of the transmitted data and retransmit the copy of old transmitted data again and again to the nodes in a particular environment thereby decreasing the residual energy level of the node and gradually the node will get destroyed due to insufficient energy. An attacker can send expired packets to the whole network environment, wasting the network resources and decreasing the lifetime of the network system. Data freshness is achieved by using nonce or a timestamp can be included with each data.

4 Attacks on WSN

The WSNs attract a number of severe attacks due to the unfriendly environment, insecure wireless communication channels, energy restrictions and various other networking circumstances. The malicious node or the attacker node when injected into the network could spread among all the neighboring nodes, potentially destroying the network, disrupting the services and taking over the control of entire network. The attacks on in WSN are generally classified into two broad categories as passive attacks-against data confidentiality and active attacks-against data confidentiality and data integrity. Furthermore, some of the important attacks are discussed in the section below:

4.1 Denial of Service Attack

This attack attempts to demolish or anesthetize all the network's resources available to its destined users either by the consumption of scarce or limited resources, alteration of configuration information or physical destruction of the network components. The two general forms of the attacks are: the ones which crash the services and the others which flood the services. The most important attacking technique is IP address spoofing with the purpose of masking or suppressing the identity of sender or mimicking the identity of another node. It results in unusually slow, interrupted network performance and the inability of the sensor node to perform its designated (proposed) functions [13].

4.2 Sybil Attack

This includes large-scale, distributed, decentralized and several other types of protocols in WSN are primarily susceptible to such attacks. Earlier known as pseudo spoofing, a particular sensor node unjustifiably claims multiple identities and resides at multiple places in the networking environment. The Sybil Attack has three orthogonal extending dimensions: direct v/s indirect communication, fabricated v/s stolen identities and simultaneity. Such type of attacks necessitates a one-to-one correspondence between the sensor nodes and their individual identities. Sybil attack can be used to initiate the attack on several types of protocols in WSN such as distributed protocols, data aggregation, misbehavior detection, voting, fair resource allocation protocols and the routing protocols [14] [15].

4.3 Blackhole Attack

The attack occurs when a compromised node appears to be more attractive in comparison to the surrounding nodes with respect to the residual energy level and the routing algorithm used, resulting in a black hole and the assemblage is known as the black hole region. The accumulated traffic that is the incoming and outgoing traffic is diverted to this region and the data packets are unable to reach to their expected destination. It also provides an opportunity for analyzing, detecting the aberrant activities and thereby applying specially designed security analysis tools to the traffic [16].

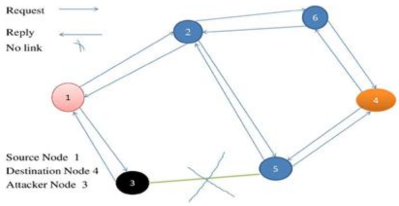


Fig. 3. Black Hole Attack.

4.4 Selective Forwarding

Selective forwarding is also known as drop-data packet attack. Any mischievous node behaving as normal nodes receives and selectively analyses different data packets. These nodes allow only few packets to pass from one node to another but on the other hand makes excuses and denies to forward certain data packets, suppresses or modifies them and eventually drops them thereby increasing the congestion and lowering the performance of network system. Such attacks happen either on the data flow or on the controlling packets and are often used in combination with the wormhole/sinkhole attacks [17].

4.5 Wormhole Attack

One of the severe attacks in wireless sensor networks specifically against the location based wireless security system since these attacks do not require compromising of any sensor nodes and could be initiated even if the system maintains authenticity, confidentiality, integrity, non-repudiation of the data transferred. The attacker records the data packets (messages/bits) at a particular individual location in the network and traverses them to another location in the network via an established link (wired or wireless). The data packets can therefore be retransmitted selectively. In a way the attacker simply fakes a route and destabilizes and interrupts the routing within the network [18].

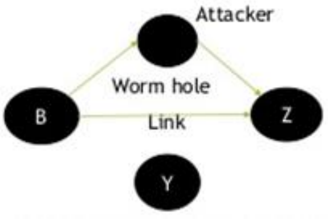


Fig. 2. Wormhole Attack.

4.6 Hello Flood Attack

This is one of the simplest and easiest Denial of Service (DOS) attack. The attacker is not an authorized node, broadcasts HELLO messages to all its neighboring authorized nodes or simply bombards a targeted node with forged requests, successful or failure connection messages, with great transmission power. A guaranteed response is expected from the receiving node which assumes the sender node to be within its normal radio frequency range. However, these attacker nodes (sender nodes) are far away from frequency range of the network. The number of packets per second increases, processing of individual nodes decreases and the system or the network gets flooded with tremendously large amount of traffic [19] [21].

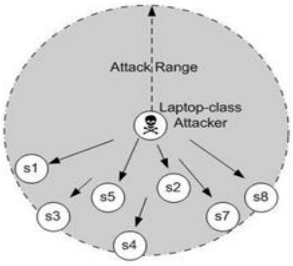


Fig. 2. Hello Flood Attack.

Table 1. Attacks on Layers and Defensive Measures.

Layers	Attacks	Defensive Measures
Physical Layer	Jamming, Tampering	Region mapping, spread-spectrum, priority messages, duty cycle, channel hopping Encryption, tamper proofing, hiding
Data Link Layer	Collision, Resource exhaustion, Unfairness	Error-correcting codes, time diversity Limited rate transmission Small frames
Network Layer	Selective Forwarding, .Spoofed routing information, Sinkhole, Wormhole, Sybil, Hello Flood	Multi-path routing, monitoring, upstream and downstream detection Egress filtering, authentication, monitoring Redundancy checking, Monitoring Authentication, probing, transmission time-based mechanism, geographical and temporal packet leashes, graphical, topological and connectivity-based approaches Trusted certification, key validation, position verification, resource testing, authentication, redundancy Verification of the bi-directionality link, signal strengthen detection, identity verification
Transport Layer	Flooding, De-synchronization	Client puzzles, rate limitation Authentication

5 Conclusions

The sensor networks are popular for mission-critical-tasks and security is immensely required for such hostile environment employed networks. Wireless sensor network is an interesting, fast emerging field in the modern scenario and provides great exposure for experimentation in the area of research and development. Through this paper, we have highlighted the four basic security issues in WSN like Confidentiality, Integrity, Robustness and Authenticity. Various constraints to the network specifically focusing on the energy constraint and some applications of sensor network have also been talked about.

The major types of attacks such as Denial of Service, Black hole, Wormhole, Hello flood attack, Sybil and Selective forwarding and their defense strategy has been discussed briefly.

References

1. G. Lu, B. Krishnamachari, and C. S. Raghavendra, "An Adaptive Energy-Efficient and Low-Latency MAC for Data Gathering in Wireless Sensor Networks," in IEEE IPDPS, 2004.
2. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications, vol. 1, no. 4, pp. 660–670, October 2002.
3. Shafiqul Abidin "Key Agreement Protocols and Digital Signature Algorithm" International Journal of Current Advanced Research, Vol 6, Issue 8, pp 5359-5362, August 2017.
4. N. Burri, P. von Rickenbach, and R. Wattenhofer, "Dozer: Ultra-Low Power Data Gathering in Sensor Networks," in ACM/IEEE IPSN, 2007.
5. Z. Jiang, J. Ma, W. Lou and J. Wu, "A Straightforward Path Routing in Wireless Ad Hoc Sensor Networks, "IEEE International Conference on Distributed Computing Systems Workshops, June 2009, pp. 103-108.
6. Shishir Bashyal and Ganesh Kumar Venayagamoorthy, "Collaborative Routing Algorithm for Wireless Sensor Network Longevity", IEEE, 2007.
7. Burrell, J.; Brooke, T.; Beckwith, R., "Vineyard computing: sensor networks in agricultural production," Pervasive Computing, IEEE, Vol. 3, No. 1, pp. 38-45, Jan-March,2004.
8. S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, "Health Monitoring of Civil Infrastructures using Wireless Sensor Networks", in ACM/IEEE IPSN, 2007.
9. M. Ceriotti, L. Mottola, G. P. Picco, A. L. Murphy, S.Guna, M. Corra, M. Pozzi, D. Zonta, and P. Zanon, "Monitoring Heritage Buildings with Wireless Sensor Networks: The Torre Aquila Deployment", in ACM/IEEE IPSN, 2009.
10. Konrad Lorincz, David Malan, Thaddeus R. F. Fulford-Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoff Mainland, Steve Moulton and Matt Welsh, "Sensor Networks for Emergency Response: Challenges and Opportunities", IEEE Pervasive Computing, Special Issue on Pervasive Computing for First Response, Oct-Dec 2004.
11. Shafiqul Abidin, "A Novel Construction of Secure RFID Authentication Protocol", International Journal of Security, Computer Science Journal, Malaysia, Vol. 8, Issue 8, pp33-36, October 2014.
12. Nouman M Durrani, Nadeem Kafi, Jawwad Shamsi, Waleej Haider and Asad M Abbsi, "Secure Multi-hop Routing Protocols in Wireless Sensor Networks: Requirements, Challenges and Solutions", IEEE, 2013.
13. Bulbenkiene, V., Jakovlev, S., Mumgaudis, and G., Priotkas, G., "Energy loss model in Wireless Sensor Networks," IEEE Digital Information Processing and communication (ICDIPC), 2012 Second International conference, PP 36-38, 10-12 July 2012.
14. J.H. Chang and L. Tassiulas, "Maximum Lifetime routing in wireless sensor networks", IEEE/ACM Transactions on Networking, Vol.12, No. 4, pp.609-619, Aug, 2004.
15. Ming Zhang, Suoping Wang, Chao Liu and Huibin Feng, "An Novel Energy-Efficient Minimum Routing Algorithm (EEMR) in Wireless Sensor Networks", IEEE, 2008.
16. Mayank Saraogi, "Security In Wireless Sensor Networks ", University of Tennessee, Knoxville.
17. Abhishek Jain, Kamal Kant and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks" 2012, Second International Conference on Advanced Computing & Communication Technologies.
18. C.Karlof & D.Wanger: Secure routing in Wireless Sensor Network: Attacks and Countermeasures. In First IEEE International Workshop on Network Protocols and Applications, pages 113-127, May 2003.
19. Manu Ahuja and Shafiqul Abidin "Performance Analysis of Vehicular Ad-hoc Network", International Journal of Computer Applications, USA, Vol 151 - No. 7, pp 28-30, October 2016.
20. Naveen Kumar, Anish Mathuria, "Improved Write Access Control and Stronger Freshness Guarantee to Outsourced Data". ICDCN 2017: 19
21. Wang, Feng, and Jiangchuan Liu. "Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches", IEEE Communications Surveys & Tutorials, 2011.

Abstract – Recently Published Articles by Faculty & Students

1. 5th Generation Wireless Communication Revolution

Shafiqul Abidin**, "5th Generation Wireless Communication Revolution", International Journal of Recent Technology and Engineering, Paper accepted for Volume - 8, Issue – 5, January 2020. (ISSN:2277-3878), Elsevier**, (Scopus Indexed).

Abstract: The entire world is moving with mobility with a ultra fast speed in utmost minimum time. This article is basically to highlight the features of future technology associated with 5G. The mobility of technology has experienced from 1 G to 4G. 5G technology is yet to come but debate has already started about its negative and positive aspects. 5 G is a complete wireless communication with almost no limitations. It supports WWWW. People say 5 G is actually Real wireless world. But all these generation have their advantages over other. 5G represent a new way of thinking. Fifth generation can be called a wearable device equipped with artificial intelligence characteristics. mindset. 5G will enable everything to be securely plus automatically monitored. In this effort has been made o discuss aspects of 5G and associated features.

2. Classifying Time-Bound Hierarchical Key Assignment Schemes

***Shafiqul Abidin et al**, "4th **Springer** International Conference on Computer, Communication and Computational Scie.nces (IC4S 2019)", Bangkok, Thailand, 11 - 12 October, 2019, Publication in Advances in Intelligent Systems and Computing (ISSN: 2194-5357), (**Scopus Indexed**)*

Abstract: Abstract. A time-bound hierarchical key assignment scheme (TBHKAS) ensures time-restricted access to the hierarchical data. There is a large number of such schemes are proposed in the literature. Crampton et. al. studied the existing hierarchical key assignment schemes in detail and classify them into generic schemes on the basis of storage and computational requirements. Such generic classification helps the implementers and researchers working in this area in identifying a suitable scheme for their work. This work studies the TBHKAS and classifies them with the same spirit. As best of our knowledge, the proposed classification captures every existing TBHKAS in the literature. Furthermore, the proposed schemes are compared and analyzed in detail.

3. B-IoT (Block Chain – Internet of Things) : A way to enhance IoT security via Block Chain against various possible attacks

***Ayasha Malik, Siddharth Gautam, Shafiqul Abidin, Bharat Bhushan' "**B-IoT (Block Chain – Internet of Things) : A way to enhance IoT security via Block Chain against various possible attacks", **IEEE** 2nd International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT – 2019), 5 - 6 July, 2019, IEEE XPLORE, (ISBN: 978-1-7281-0283-23), (**Scopus Indexed**).*

Abstract: In contrast with past, the blooming of Internet of Things is enlarging swiftly. But providing security in IoT devices is still a challenging issue and the solution is "Blockchain". Blockchain is a synthesistechnology that integrates an innovative and well-built eye-sight tomould all-inclusive clarification to IoT device securities. Blockchain is used to furnish IoT device in a way of security, as it fixed a route to modify our job by cloud build evolution. Blockchainis speedily growing to be the upcoming interrupted revolution for securedconnection or association, hopefully provide positive changes towards our working and living upcoming century.

4. Enhancing Security in WSN by Artificial Intelligence

Shafiqul Abidin, "Springer *International Conference on Intelligent Data Communication and Internet of Things (ICICI - 2018)****", Chapter 93 , Lecture Notes on Data Engineering and Communication Technologies*** *Series ISSN : 2367-4512, ISSN: 2367-4520 (Electronic), ISBN: 978-3-030-03145-9, ISBN : 978-3-030-03146-6 (ebook), pp 814-821, January 2019,* ***(Scopus Indexed)***

Abstract: Wireless sensor network (WSN) comprises of sensor nodes such as magnetic, thermal, infra red, and the radar is setup in a particular geographical area. These nodes are used to transmit data or packet from one node to another i.e., from sender to receiver. The capabilities of WSN include manipulating and controlling the physical and environmental entities such as – humidity, temperature, sound, pressure, light etc. Wireless Sensor Networks have various applications such as Military applications, Healthcare applications etc. and also the security of the wireless sensor network is becoming a major concern. There are various types of attacks that are performed on wireless sensor networks. So due to this it is necessary to prevent WSN against these types of attacks. The size of the sensor node is small. The sensor nodes are energy constraints. The sensor nodes can easily be operated on low power. Basically, this paper presents a system which is used to prevent WSN from various types of attacks. By using the concept of artificial intelligence, we can easily detect the malicious nodes so that we can easily prevent our secret information from malicious nodes and also on expert system is developed using C language to prevent WSN from various types of attacks.

5. Centralised Operating System- A new way to secure the computer networks

Shafiqul Abidin *and* ***Mohini Chauhan,*** *"Centralised Operating System - A new way to secure the computer networks",* ***IEEE*** *International Conference on New Trends in Engineering & Technology (ICNTET 2018 – Conference # 44368), Chennai , Tamil Nadu, India, IEEE Xplore , ISBN : 978-1-5386-5630-3 and 978-1-5386-5629-7, 7-8 September, 2018,* ***(Scopus Indexed).***

Abstract: The risk of any computer's compromizsation is most common and this often let others in trouble. Making a system completely isolated from many functions that are somewhat connect to vulnerability and threats can be disconnect from it to some extent. The idea behind this technology is to make system depend on a center or a master system so that the cost of security and the resources can be more specific and

effective. This will comprise of 'Star Topology' and hence all the command control be totally depend on the master computer.

6. CMOS CMOS Realization of Electronically tunable Grounded Inductor Application Band Pass Amplifier Design for Noise Minimization in RF System

Shafiqul Abidin et al, *"CMOS Realization of Electronically tunable Grounded Inductor Application Band Pass Amplifier Design for Noise Minimization in RF System", IEEE International Conference on Inventive Computation Technologies (ICICT - 2018),* ***IEEE Xplore*** *, ISBN : 978-1-5386-4985-5, and 978-1-5386-4984-8, November, 2018, (****Scopus Indexed)***

Abstract: We present grounded Inductor based band-pass Amplifier to minimize the noise with the degenerative feedback resistance technique in common source and common gate configuration of MOS Transistor. The thermal noise of the proposed MOS Transistor architecture is reduced noise by using input feedback stage with a degeneration resistor in the common source and common gate configuration. RF Band Pass Amplifier which has grounded inductor, low-noise amplifiers (LNA) and An Radio Frequency (RF) band-pass filter (BPF) for proposed RF System to minimize the noise with .18µm as well as CMOS 90 nm technology. The quality factor obtained at maximum resonant frequency which are 4.0 - 4.4 at 3.849 GHz respectively. The tuning frequency range at 3.43 GHz- 3.849 GHz, and the band pass filter parameters yield total power consumption of 0.81mW - 1.46 MW, at low noise figure of 4.2 dB - 5.4 dB with the low noise sensitivity 3.10µm- 3.13µm . The inductors are simulated by active elements namely Voltage Differencing Voltage trans conductance Amplifier (VDVTA) and Gyrator C are key features in Radio Frequency Integrated Circuits.

7. Human Injectable Chip: A novel approach for secure data transmission in media

Mohini Chauhan, *"Human Injectable Chip: A novel approach for secure data transmission in media", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT 2019), (****Scopus Indexed****)*

Abstract: Since everything is embedded with the rays that are making the connection with the chip and the connected devices, it become very important to focus on the powering system for the chip battery. We will see the way in which this battery is powering itself and this is something unique by the term of powering source. Another threat comes to my mind is regarding the attack that can happen in middle of the process. The rays passing through the air can be intercept by a third party in order to steal the information. To prevent this, we will minimize the use of internet as much as possible by making everything to store the information physically. We will later see how this info will be store on the device finally by using internet.

8. Performance Evaluation of Pigeon Bird Classification Techniques using Template Matching

Monika *and* ***Himanshi Singh,*** *"Performance Evaluation of Pigeon Bird Classification Techniques using Template Matching", CiiT AIML*

Abstract : So as to update the pigeon feathered creature grouping, perceive flying creatures and assent their conduct is an absolute necessity prerequisite. This examination paper is showing a strategy towards improvement of pigeon fledgling acknowledgment approaches. Flying creature's dataset is made through 2D pictures by creating highlight vector of feathered creatures utilizing different picture preparing procedures so as to separate the winged animal bends from nature. According to the examinations head is a most particular piece of fowls, various highlights are separated utilizing format coordinating and make it ready to perform characterization of pigeon winged animal between various sorts of feathered creatures. Flying creatures basically have three sorts of practices: rummaging conduct, carefulness conduct and flight conduct. Flying creatures may search for nourishment and get away from the predators by the social cooperation's to get a high possibility of survival. By demonstrating these social practices, social collaborations and the related fowl's knowledge, four hunt methodologies related with five disentangled principles are detailed in a calculation. Recreations and examinations dependent on eighteen benchmark issues exhibit the adequacy, predominance and steadiness of algorithm. A few propositions for future research are additionally talked about.

Achievements – Department of Information Technology

- Mr D K Mishra has been conferred "Dr Rajendra Prasad Award - 2019", for meritous achievements in the field of education and commitment of teaching by International Eminent Educationists' Forum of India.
- Dr Shafiqul Abidin's research article "Controlling Device by IoT" has been accepted by IJRTE –Elsevier Journal.
- Mr Siddharth Gautam got best paper presentation Award in IEEE Conference "ICSPC – 2019".
- Mr Siddharth Gautam got best paper presentation Award in Springer Conference International Conference in Pattern & Recognition.
- Tanmay Singla (B Tech - 3rd Year) has been playing in State Level Cricket Tournaments.
- Mr Siddharth Gautam chaired a session in IEEE Conference, Sharda University. Greater Noida, 2019.
- One of scholars has been awarded Ph D Degree under the supervision of Dr Shafiqul Abidin.
- Rachit Mann got admission in M Tech – Delhi Technical University.
- Pratiksha Sharma got admission in M Tech – Indira Gandhi Delhi Technical University for Women (IGDTUW).
- Atul Aman got admission in M Tech – Delhi Technical University.
- Aditya Malik has joined Yellow Messenger, Bangalore with a annual package of ₹25 Lakh.
- Tanish Kaushal has been selected in GGSIP University Cricket Team. He is playing in North India Inter-University Cricket Tournament 2019. His performance has been appreciated by coach and team members.