University of Mohamed Khider Biskra
Faculty of Sciences and Technology
Electrical Engineering Department

MASTER'S THESIS

Sciences and Technology
Branch: Telecom
Option: network telecom
Ref.: …………..

Presented and Prepared by:
Ounoki amira Bouchareb rayane

On: 23/juin/2022

CNN in Deep Learning for WAN Wireless Network Security Using CDMA

Jury:

Dr.	Baarir zinedine	**Pr**	**University of Biskra**	**President**
Dr.	Zehani soraya	**MCA**	**University of Biskra**	**Examiner**
Dr.	Toumi abida	**Pr**	**University of Biskra**	**Supervisor**
Dr.	Betka Abir	**Dr**	**University of Biskra**	**Co.Supervisor**

Academic Year: 2021 – 2022

University of Mohamed Khidar Biskra
Faculty of Sciences and Technology
Electrical Engineering Department

MASTER’S THESIS

Sciences and Technology
Branch: Telecom
Option: network Telecom

Theme:

CNN in Deep Learning for WAN Wireless Network Security Using CDMA

Presented by:

Ounoki amira

Bouchareb rayane

Favorable opinion of the supervisor:

Pr. TOUMI

Favorable opinion of the Jury President:
Pr. Baarir Zinedine

Stamp and signature

Acknowledgment

First foremost, praises and thanks to Allah, the Almighty, for His showers of blessings throughout my research work to complete this thesis successfully.

We would like sincerely thank our supervisor Pr.Toumi. A. as well as our co-supervisor Dr.Betka.A for his advice and encouragement, which enabled us to carry out this work in the best conditions.

We sincerely thank the members of the jury for agreeing to review and evaluate our work, Pr. Baarir. Z being the president and Dr. Zehani. S being only an examiner.

We also express our gratitude to all the professors and teachers who have collaborated in our formation from our first cycle of study until the end.

Without forgetting of course to deeply thank all those who contributed directly or indirectly to the realization of this work.

THANK YOU ALL

Dedication

I am glad to have the opportunity to dedicate this work from the bottom of my heart to my dear:

My dear parents who stayed day and night to provide everything I need for an honorable and successful life, you are my role model and the light of my eyes.

My dear, brothers **Said** and **Okba,** my sisters **Sarah**, **Serine** and **Soha,** and I will not forget my older sister, **Lamis** and her daughter **Zina**, you are my helper and the source of my pride.

Greetings from me to every family, **Ounoki** and the **Zitouni** family.

Dear teachers and everyone who has taught me something all my life, I owe you all the successes that I have had or will have.

My dear friends, especially " **Tayeb Sofiane** and **Sif Eddine Boudjellal** and **Bouchareb Rayane**", you are the source of my happiness. I thank you for every smile you put on my face.

Ounoki_Amira

Dedication

I dedicate this humble work: To my dear parents

For having them by my side all my life, and who believed in me during my educational and university cycle. May they find here the testimony of my deepest love and surest gratitude.

To my brother **Moundji,** my sisters **Soumia**, my older sister **Aya,** her daughter **Miral**, and the **twins Amin and Mouhamed**

And to all the **Bouchareb** family and the **Guerbaz** family

And to all my friends, my sister and my friend **Amira Ounoki, Ben Aishi Moufida , bin Mebark Mebarka and Bouzidi chaima**, and I will not forget my friend and my right arm **Fraih Lakhder**

May God protect them from all pain and fate.

Bouchareb_ Rayane

University of Mohamed Khider Biskra
Faculty of Sciences and Technology
Département of génie électrique

MASTER'S THESIS

Sciences and Technology
Branch: Telecom
Option: Network telecom

Theme:

CNN in Deep Learning for WAN Wireless Network Security Using CDMA

Abstract

Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. It is subset of network security that add protection for a wireless computer network.The aim of this study is to design a model capable of predicting the probability of attacks in networks with maximum accuracy. Classification algorithms are widely used in the wireless networks field to classify data into different categories according to some that relatively restrict the individual classifier. Therefore, one deep learning classification algorithm (Convolutional Neural Networks (CNNs)), have been used in this experiment to detect attacks at an as soon as possible. The experiments performed on database.

The performance of the algorithm evaluated on different scales such as accuracy, loss, noise, BER, changing in the values of SNR.

The results of the first part obtained from the database showed that CNN algorithm achieved with the highest accuracy of 99.1%.

In the second part, the results obtained from the same database it showed that after using the CDMA technique, deep learning removed the intruder, and it gave a good result.

Keywords: SNR (Signal-to-noise ratio), **CNN** (Convolution Neural Network), **BER** (bit error rate), **CDMA** (code division multiple Access)

Résumé

La sécurité des réseaux sans fil est le processus de conception, de mise en œuvre et d'assurance de la sécurité sur un réseau informatique sans fil. Il s'agit d'un sous-ensemble de sécurité réseau qui ajoute une protection pour un réseau informatique sans fil

Le but de cette étude est de concevoir un modèle capable de prédire la probabilité d'attaques dans les réseaux avec un maximum de précision. Les algorithmes de classification sont largement utilisés dans le domaine des réseaux sans fil pour classer les données en différentes catégories selon certaines qui restreignent relativement le classificateur individuel. Par conséquent, un algorithme de classification d'apprentissage profond (réseaux de neurones convolutifs (CNN)) a été utilisé dans cette expérience pour détecter les attaques le plus tôt possible. Les expériences réalisées sur base de données.

Les performances de l'algorithme sont évaluées sur différentes échelles telles que la précision, la perte, le bruit, le BER, l'évolution des valeurs de SNR.

Les résultats de la première partie obtenus à partir de la base de données ont montré que l'algorithme CNN atteint la plus grande précision de 99,1 %.

Dans la deuxième partie, les résultats obtenus à partir de la même base de données ont montré qu'après avoir utilisé la technique CDMA, l'apprentissage en profondeur a éliminé l'intrus, et cela a donné un bon résultat.

Mots-clés : SNR (Rapport signal sur bruit), **CNN** (Convolution Neural Network), **BER** (bit error rate), **CDMA** (Code Division Multiple Access)

الملخص

أمان الشبكة اللاسلكية هو عملية تصميم وتنفيذ وضمان الأمن على شبكة كمبيوتر لاسلكية. إنها مجموعة فرعية من أمان الشبكة تضيف حماية لشبكة كمبيوتر لاسلكية, الهدف من هذه الدراسة هو تصميم نموذج قادر على التنبؤ باحتمالية الهجمات في الشبكات بأقصى قدر من الدقة .تُستخدم خوارزميات التصنيف على نطاق واسع في مجال الشبكات اللاسلكية لتصنيف البيانات إلى فئات مختلفة وفقًا لبعض الفئات التي تقيد المصنف الفردي نسبيًا. لذلك، تم استخدام خوارزمية تصنيف التعلم العميق) الشبكات العصبية التلافيفية ((CNN)في هذه التجربة لاكتشاف الهجمات في أسرع وقت ممكن. التجارب التي أجريت على قاعدة البيانات.

تم تقييم أداء الخوارزمية على مستويات مختلفة مثل الدقة، والخسارة، والضوضاء، وBER، وتغيير قيم.SNR

أظهرت نتائج الجزء الأول التي تم الحصول عليها من قاعدة البيانات أن خوارزمية CNN حققت أعلى دقة بلغت 99.1٪.

في الجزء الثاني، أظهرت النتائج التي تم الحصول عليها من نفس قاعدة البيانات أنه بعد استخدام تقنيةCDMA ، أزال التعلم العميق الدخيل، وأعطى نتيجة جيدة.

الكلمات الرئيسية: SNR (نسبة الإشارة إلى الضوضاء)، **CNN** (شبكة عصبية تلافيفية)، **BER** (معدل خطأ بت)، **CDMA** (وصول متعدد بتقسيم الكود)

Table of Content:

List of Figures

Chapter I: Machine Learning & Deep Learning

Chapter II: Wireless Network Security

Chapter III: Wireless Network Attack Predictive System

List of Table

Chapter I: Machine Learning & Deep Learning

Chapter II: Wireless Network Security

Chapter III: Wireless Network Attack Predictive System

List of Abbreviation

Chapter I	*Chapter II*	**Chapter III**
ML: machine learning. **DL:** Deep Learning. **AI:** Artificial Intelligence. **SVM:** Support Vector Machine. **KNN:** K-Nearest Neighbors. **ANN:** Artificial Neural Network. **API:** Application Programming Interface. **CNN:** Convolution Neural Network. **RNN:** Recurrent Neural Network. **CPU:** Central Processing Unit. **GPU:** Gated Recurrent Unit **LSTM:** Long Short-Term Memory. **URL:** Uniform Resource Locator. **DNN:** Deep Neural Network. **SLP:** Single Layer Perceptron. **MLP:** Multilayer Perceptron. **RBM:** Restricted Boltzmann Machine. **DBM:** Deep Boltzmann Machine. **DBNs:** Deep Belief Networks.	**OSI:** Open Systems Interconnection. **WPAN:** Wireless Personal Area Network. **WLAN:** Wireless Local Area Network. **WMAN:** Wireless Metropolitan Area Network. **WWAN:** Wireless Wide Area Network. **RF:** Radio Frequency. **GSM:** Global System for Communication. **GPRS:** General Packet Radio Service. **UMTS:** Universal Mobile Telecommunication System. **W-CDMA:** Wide- Code Division Multiple Access. **WEP:** Wired Equivalent Privacy. **WPA:** Wi-Fi Protected Access. **TKIP:** Temporary Key Integrity Protocol . **AES:** Advanced Encryption Standard. **PSK:** Pre-shared Key. **AP:** Access Point. **VPNs:** Virtual Private Networks. **DOS:** Denial of Service. **EAP:** Extensible Authentication Protocol. **SSID:** Service Set Identifier. **FDMA:** Frequency Division Multiple Access . **TDMA:** Time Division Multiple Access. **CDMA :** Code Division Multiple Access.	**AM-DSB:** double sideband with carrier AM. **AM-SSB:** Single-sideband. **WB-FM:** Wideband FM. **8PSK:** 8 Phase-shift keying. **BPSK:** Binary phase-shift keying. **CPFSK:** Continuous-phase frequency-shift keying. **GFSK:** Gaussian frequency-shift keying. **4PAM:** 4 Pulse Amplitude Modulation. **16QAM :** 16Quadrature amplitude modulation. **64QAM:** 64Quadrature amplitude modulation. **QPSK:** Quadrature phase shift keying. **SNR:** signal-to-noise ratio. **BER:** Bite Error Rtae.

General Introduction:

Artificial intelligence (AI) is a technology designed after using multiple layers of information – including algorithms, pattern matching, rules, deep learning and cognitive calculations – to understand data. It found today in computers social networks, transport and wireless networks. The application of AI in wireless network allowing analyzing the data and providing estimates. With the aim of predicting many attacks so that devices can intervene as quickly as possible to reduce the risk of attacks on network security, Deep learning or deep learning a type of artificial intelligence derived from machine learning (automatic learning) where the machine is able to learn by itself. Through this Master's thesis, we will be interested in the use of an algorithm of several deep learning algorithms for the prediction of wireless network attacks, which are a failure of the network security system. Our problem allows us to define the study of network security as a classification process and the use of IT is becoming more and more frequent to implement this classification although is the most important factor in the study. The method used in this work is the application of CNN classification algorithm and using many, digital and analog modulations to a single database In addition to dividing the networks into three sections (inside the network outside the network and intruder on the net) then apply a CDMA protocol. Finally, we have improved the classification with the CNN algorithm and come out with good results and with the use of CDMA that transmits the signals to the desired destination at the same frequency and at the same time by encoding.

The outline of this work organized into three main chapters as follows:

Chapter 1: an overview of artificial intelligence, and presentation of a general overview of machine learning, their different type.

Chapter 2: Presentation of wireless networks, and their type, how to protect it, access method (CDMA).

Chapter 3: a technical study in which we define the software environment used to build our application, then a detailed definition on the databases used; the results presented, compared and interpreted

Chapter I

Machine Learning & Deep Learning

I.1 Introduction:

Before we get to what Machine Learning (ML) and Deep Learning (DL) is, we need to introduce the concept of Artificial Intelligence.

Artificial Intelligence (AI) is a vast field, where we try to mimic human behavior with the aim of making machines so powerful to perform many kinds of tasks such as problem solving, knowledge representation, voice recognition, and others. The basic idea is to put knowledge into the machine.

Machine learning and deep learning are part of artificial intelligence. Both of these approaches result in the ability to make intelligent decisions.

The relationship between the three concepts IA, ML and DL summarized by the authors in the following figure:

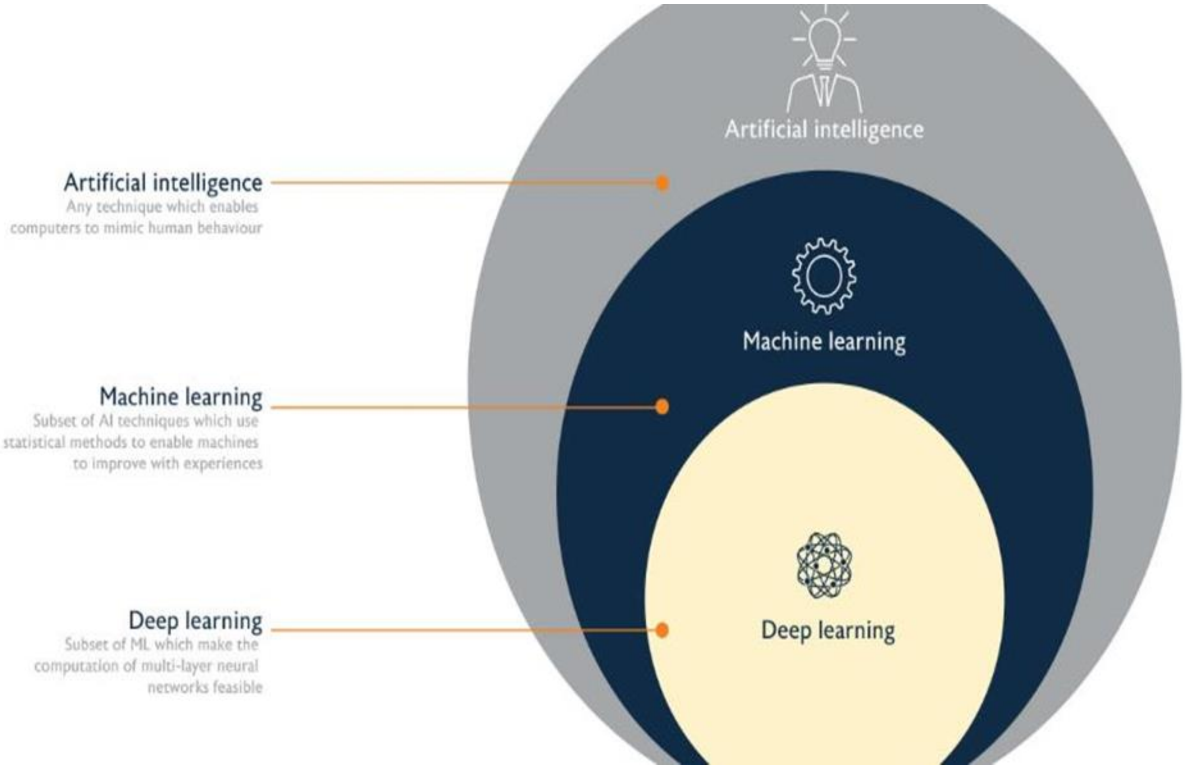

Artificial intelligence
Artificial intelligence
Any technique which enables computers to mimic human behaviour
Machine learning
Machine learning
Subset of AI techniques which use statistical methods to enable machines to improve with experiences
Deep learning
Deep learning
Subset of ML which make the computation of multi-layer neural networks feasible

Figure I.1: The relationship between AI, ML and DL**.**

I.2 Machine learning:

I.2.1 Definition:

Machine Learning (ML) is a sub-field of Artificial Intelligence (AI) which concerns with developing computational theories of learning and building learning machines. The goal of machine learning, closely coupled with the goal of AI, is to achieve a thorough understanding about the nature of learning process (both human learning and other forms of learning), about the computational aspects of learning behaviors, and to implant the learning capability in computer systems. Machine learning has been recognized as central to the success of Artificial Intelligence, and it has applications in various areas of science, engineering and Society. [23]

I.2.2 The different types of machine learning:

At a high-level, machine learning is simply the study of teaching a computer program or algorithm how to progressively improve upon a set task that it is given on the research-side of things, machine learning can be viewed through the lens of theoretical and mathematical modeling of how this process works, however more practically it is the study of how to build applications that exhibit this iterative improvement there are many ways to frame this idea, but largely there are three major recognized categories: supervised learning, unsupervised learning, and reinforcement learning. [25]

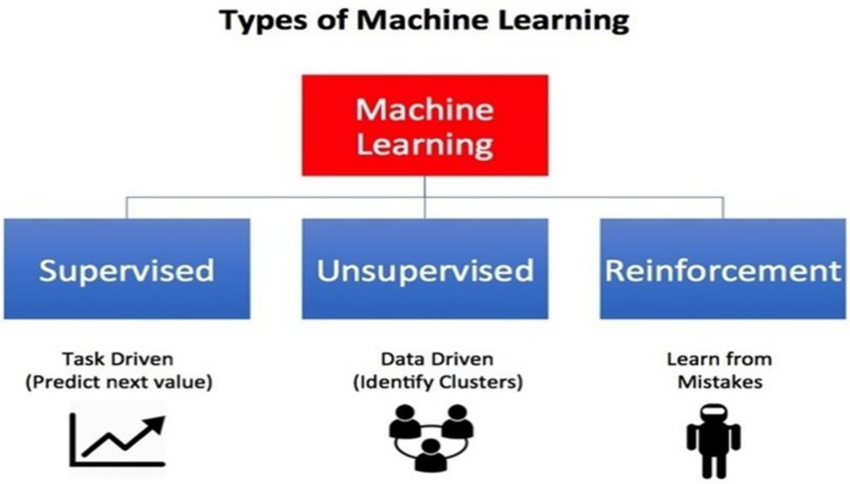

Types of Machine Learning
Machine Learning
Supervised
Unsupervised
Reinforcement
Task Driven (Predict next value)
Data Driven (Identify Clusters)
Learn from Mistakes

Figure I.2: types of machine learning.

I.2.2.1 Supervised Learning:

Supervised learning is analogous to training a child to walk. You will hold the child's hand, show him how to take his foot forward, walk yourself for a demonstration and so on, until the child learns to walk on his own [18].

In this type of machine-learning system, the data that you feed into the algorithm, with the desired solution, referred to as "labels."[21].

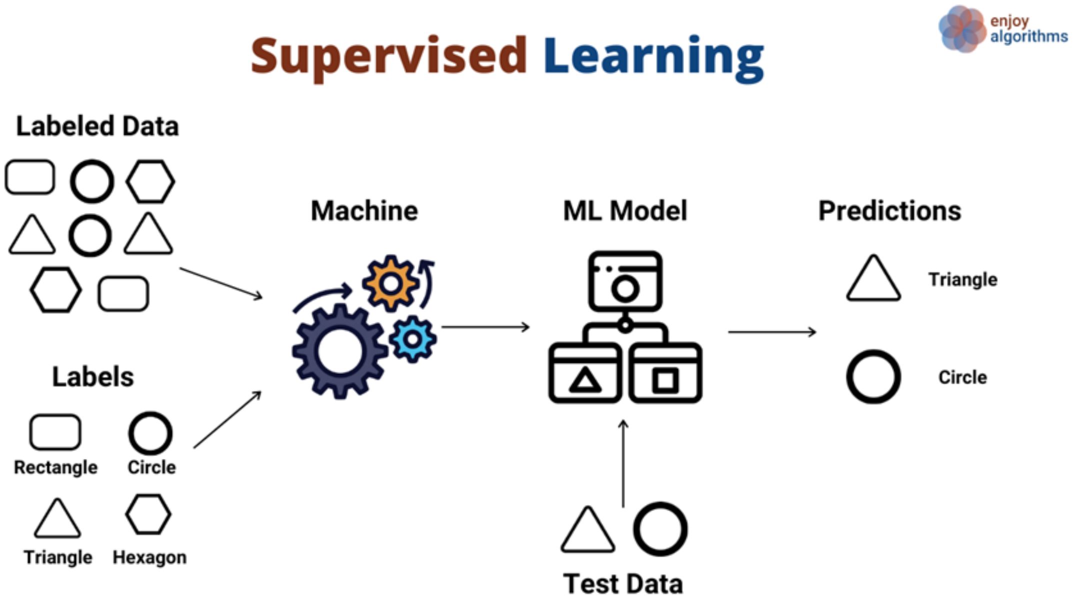


Figure I.3: supervised learning training.

- **Regression:**

Similarly, in the case of supervised learning, you give concrete known examples to the computer. You say that for given feature value x1 the output is y1, for x2 it is y2, for x3 it is y3 and so on, based on this data, you let the computer figure out an empirical relationship between x and y.

Once the machine trained in this way with a sufficient number of data points, now you would ask the machine to predict Y for a given X. Assuming that you know the real value of Y for this given X, you will be able to deduce whether the machine's prediction is correct.

Thus, you will test whether the machine has learned by using the known test data. Once you are satisfied that the machine is able to do the predictions with a desired level of accuracy (say 80 to 90%) you can stop further training the machine.

Now, you can safely use the machine to do the predictions on unknown data points, or ask the machine to predict Y for a given X for which you do not know the real value of Y. This training comes under the regression that we talked about earlier.

- **Classification:**

You may also use machine-learning techniques for classification problems. In classification problems, you classify objects of similar nature into a single group. For example, in a set of 100 students say, you may like to group them into three groups based on their heights - short, medium and long. Measuring the height of each student, you will place him or her in a proper group.

Supervised Learning was applied successfully in several cases; several algorithms have been developed for supervised learning [18].

The most important supervised algorithms:

- K-nears neighbors.
- Linear regression.
- Support vector machines neural networks.
- Logistic regression.
- Decision trees and random forests.

I.2.2.2 Unsupervised Learning:

In unsupervised learning, we do not specify a target variable to the machine; rather we ask machine “What can you tell me about X? More specifically, we may ask questions such as given a huge data set X, “What are the five best groups we can make out of X?” or “What features occur together most frequently in X?. To arrive at the answers to such questions, you can understand that the number of data points that the machine would require to deduce a strategy would be very large. In case of supervised learning, the machine can trained with even about few thousands of data points. However, in case of unsupervised learning, the number of data points that reasonably accepted for learning starts in a few millions. These days, the data is generally abundantly available. The data ideally requires curating. However, the amount of data that is continuously flowing in a social area network, in most cases data curation is an impossible task.

Because unsupervised learning is based upon the data and its properties, we can say that unsupervised learning is data-driven. The outcomes from an unsupervised learning task are controlled by the data and the way its formatted. Some areas you might see unsupervised learning crop up are:

- **Recommender Systems:**

  If you have ever used YouTube or Netflix, you have most likely encountered a video recommendation system. These systems are often times placed in the unsupervised domain. We know things about videos, maybe their length, their genre, etc. We also know the watch history of many users. Taking into account users that have watched similar videos as you and then enjoyed other videos that you have yet to see, a recommender system can see this relationship in the data and prompt you with such a suggestion.

- **Buying Habits:**

It is likely that your buying habits are contained in a database somewhere and that data is being bought and sold actively at this time. These buying habits can be used in unsupervised learning algorithms to group customers into similar purchasing segments. This helps companies market to these grouped segments and can even resemble recommender systems.

- **Grouping User Logs:**

Less user facing, but still very relevant, we can use unsupervised learning to group user logs and issues. This can help companies identify central themes to issues their customers face and rectify these issues, through improving a product or designing an FAQ to handle common issues.

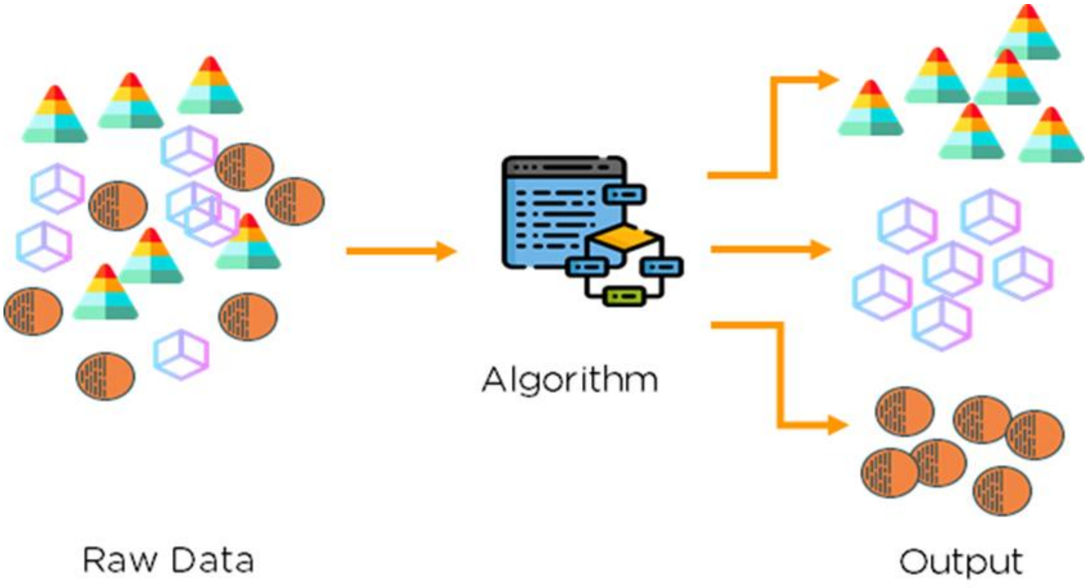


Figure I.4: Unsupervised Learning.

The most important unsupervised algorithms:

- Clustering: k- means, hierarchical cluster analysis
- Association rule learning: Eclat, apriority.
- Visualization and dimensionality reduction: kernel PCA, t-distributed PCA [21].

I.2.2.3 Reinforcement Learning:

Reinforcement Learning defined as a Machine Learning method that is concerned with how software agents should take actions in an environment. Reinforcement Learning is a part of the deep learning method that helps you to maximize some portion of the cumulative reward.

This neural network learning method helps you to learn how to attain a complex objective or maximize a specific dimension over many steps [26].

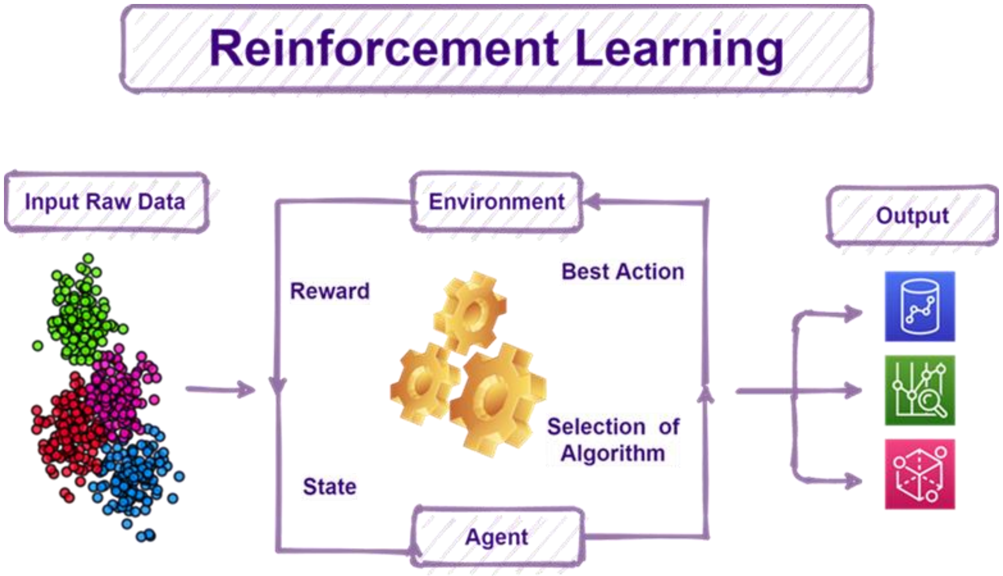


Figure I.5: Reinforcement Learning

The most important reinforcement algorithms:

- Q learning.
- Policy iteration.
- Value iteration [27].

I.2.3 Machine learning algorithms:

I.2.3.1 Linear Regression:

To understand the working functionality of this algorithm, imagine how you would arrange random logs of wood in increasing order of their weight. There is a catch; however – you cannot weigh each log. You have to guess its weight just by looking at the height and girth of the log (visual analysis) and arrange them using a combination of these visible parameters. This is what linear regression in machine learning is like.

In this process, a relationship established between independent and dependent variables by fitting them to a line. This line is known as the regression line and represented by a linear equation Y= a *X + b.

In this equation:

- Y – Dependent Variable

- a – Slope
- X – Independent variable
- b – Intercept

The coefficients a & b are derived by minimizing the sum of the squared difference of distance between data points and the regression line.

I.2.3.2 Logistic Regression:

Logistic Regression is used to estimate discrete values (usually binary values like 0/1) from a set of independent variables. It helps predict the probability of an event by fitting data to a logit function. It is also called log it regression.

These methods listed below are often used to help improve logistic regression models:

- Include interaction terms.
- Eliminate features.
- Regularize techniques.
- Use a non-linear model.

I.2.3.3 Naive Bayes Algorithm:

A Naive Bayes classifier assumes that the presence of a particular feature in a class is unrelated to the presence of any other feature.

Even if these features related to each other, a Naive Bayes classifier would consider all of these properties independently when calculating the probability of a particular outcome.

A Naive Bayesian model is easy to build and useful for massive datasets. It is simple and known to outperform even highly sophisticated classification methods.

I.2.3.4 K-Means:

It an unsupervised learning algorithm that solves clustering problems. Data sets are classified into a particular number of clusters (let is call that number K) in such a way that all the data points within a cluster are homogenous and heterogeneous from the data in other clusters.

How K-means forms clusters:

- The K-means algorithm picks k number of points, called centroids, for each cluster.
- Each data point forms a cluster with the closest centroids, i.e., K clusters.
- It now creates new centroids based on the existing cluster members.
- With these new centroids, the closest distance for each data point is determined. This process repeated until the centroids do not change.

I.2.3.5 Random Forest Algorithm:

A collective of decision trees called a Random Forest. To classify a new object based on its attributes, each tree is classified, and the tree "votes" for that class. The forest chooses the classification having the most votes (over all the trees in the forest).

Each tree planted & grown as follows:

- If the number of cases in the training set is N, then a sample of N cases taken at random. This sample will be the training set for growing the tree.
- If there are M input variables, a number m<<M is specified such that at each node, m variables are selected at random out of the M, and the best split on this m is used to split the node, The value of m is held constant during this process.
- Each tree grown to the most substantial extent possible. There is no pruning.

I.2.3.6 SVM (Support Vector Machine) Algorithm:

SVM algorithm is a method of classification algorithm in which you plot raw data as points in an n-dimensional space (where n is the number of features you have). The value of each feature then tied to a particular coordinate, making it easy to classify the data. Lines called classifiers can be used to split the data and plot them on a graph.

I.2.3.7 Decision Tree:

Decision Tree algorithm in machine learning is one of the most popular algorithm in use today; this is a supervised learning algorithm that is used for classifying problems. It works well classifying for both categorical and continuous dependent variables. In this algorithm, we split the population into two or more homogeneous sets based on the most significant attributes/ independent variables.

I.2.3.8 KNN (K- Nearest Neighbors) Algorithm:

This algorithm can be applied to both classification and regression problems. Apparently, within the Data Science industry, it is more widely used to solve classification problems. it is a simple algorithm that stores all available cases and classifies any new cases by taking a majority vote of its k neighbors. The case then assigned to the class with which it has the most in common. A distance function performs this measurement.

KNN can be easily understood by comparing it to real life. For example, if you want information about a person, it makes sense to talk to his or her friends and colleagues!

Things to consider before selecting K Nearest Neighbors Algorithm:

- KNN is computationally expensive
- Variables should be normalized, or else higher range variables can bias the algorithm Data still needs to be pre-processed.

I.2.3.9 Dimensionality Reduction Algorithms:

In today's world vast amounts of data are being stored and analyzed by corporates government agencies and research organizations, this raw data contains a lot of information - the challenge is in identifying significant patterns and variables.

Dimensionality reduction algorithms like Decision Tree, Factor Analysis, Missing Value Ratio, and Random Forest can help to find relevant details.

I.2.3.10 Gradient Boosting Algorithm and Ada Boosting Algorithm:

These are boosting algorithms used when massive loads of data have to be handled to make predictions with high accuracy. Boosting is an ensemble-learning algorithm that combines the predictive power of several base estimators to improve robustness.

In short, it combines multiple weak or average predictors to build a strong predictor. These boosting algorithms always work well in data science competitions like Kaggle, AV Hackathon, and CrowdAnalytix. These are the most preferred machine learning algorithms today. Use them, along with Python and R Codes, to achieve accurate outcomes [32].

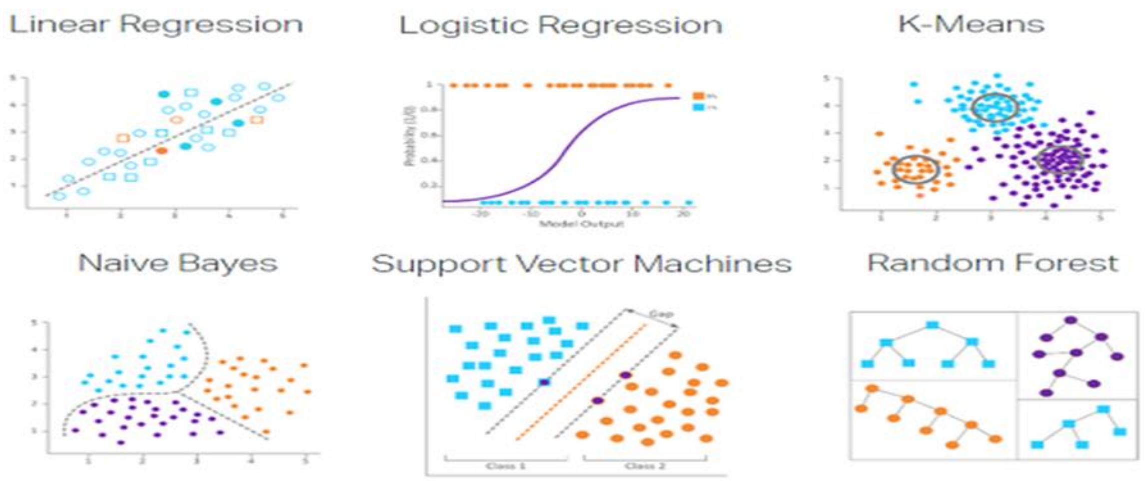


Figure I.6: Machine-learning algorithms.

I.3 Deep learning

I.3.1 Definition:

Deep learning is a set of learning methods attempting to model data with complex architectures combining different non-linear transformations. The elementary bricks of deep learning are the neural networks that combined to form the deep neural networks. These techniques have enabled significant progress in the fields of sound and image processing, including facial recognition, speech recognition, computer vision, automated language processing, text classification (for example spam recognition).[1]

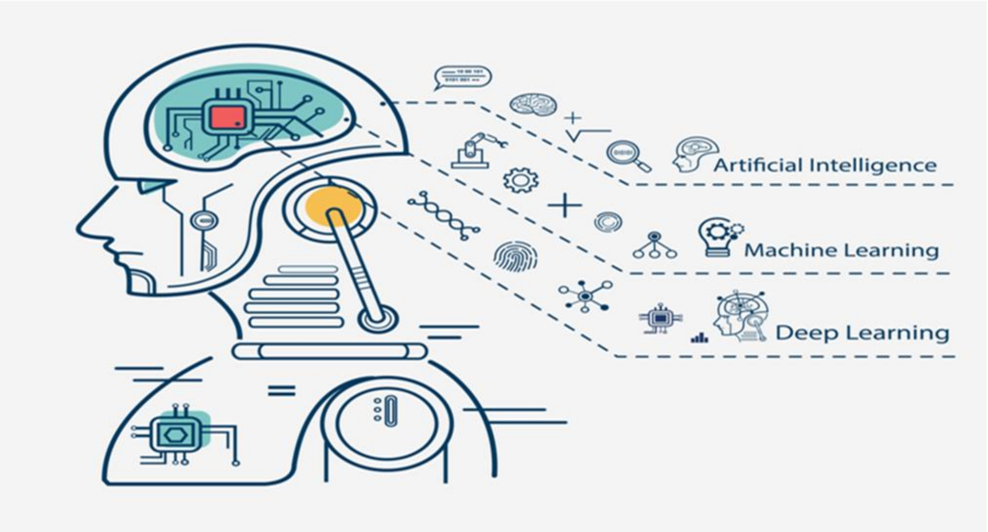


Figure I.7: Definition Deep Learning.

✓ why choose deep learning:

Deep learning eliminates some of data pre-processing that is typically involved with machine learning. These algorithms can ingest and process unstructured data, like text and images, and it automates feature extraction, removing some of the dependency on human experts.

I.3.2 Evolution of Deep Learning:

First Generation of Artificial Neural Networks (ANN) was composed of perceptron in neural layers, which were limited in computations. The second generation calculated the error rate and back propagated the error. Restricted Boltzmann machine overcame the limitation of back propagation, which made the learning easier. Then other networks evolved eventually, figure illustrates a timeline showing the evolution of deep models along with the traditional model. The performance of classifiers using deep learning improves on a large scale with an increased quantity of data when compared to traditional learning methods. Figure depicts the performance of traditional machine learning algorithms and deep learning algorithms.

The performance of traditional machine learning algorithms becomes stable when it reaches the threshold of training data whereas the deep learning upturns its performance with increased amount of data. Now a day's deep learning used in a lot many applications such as Google's voice and image recognition, Netflix and Amazon's recommendation engines, Apple's Siri, automatic email and text replies, catboats etc...[3]

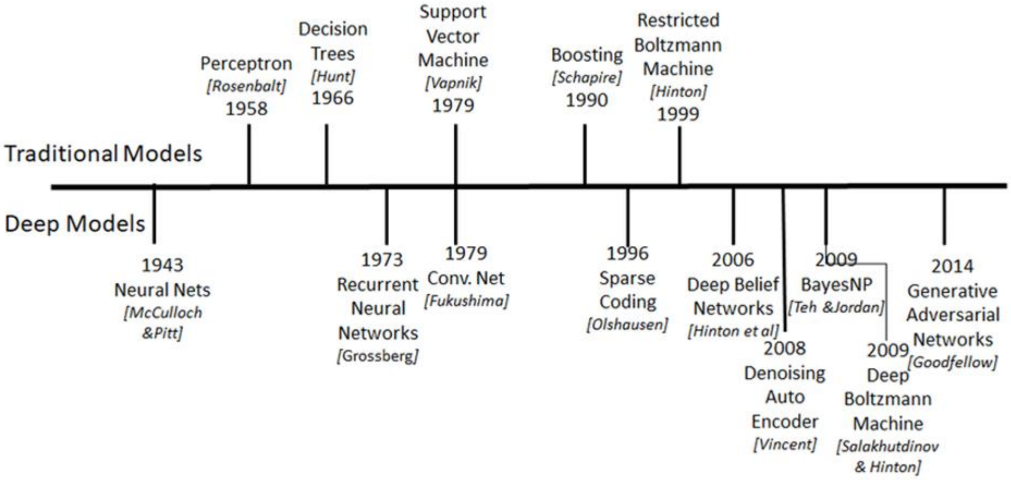

Perceptron [Rosenbalt] 1958
Decision Trees [Hunt] 1966
Support Vector Machine [Vapnik] 1979
Boosting [Schapire] 1990
Restricted Boltzmann Machine [Hinton] 1999
Traditional Models
Deep Models
1943 Neural Nets [McCulloch &Pitt]
1973 Recurrent Neural Networks [Grossberg]
1979 Conv. Net [Fukushima]
1996 Sparse Coding [Olshausen]
2006 Deep Belief Networks [Hinton et al]
2008 Denoising Auto Encoder [Vincent]
2009 BayesNP [Teh &Jordan]
2009 Deep Boltzmann Machine [Salakhutdinov & Hinton]
2014 Generative Adversarial Networks [Goodfellow]

Figure I.8: Evolution of Deep Models.

I.3.3 Deep learning methods:

I.3.3.1 Back propagation:

While solving an optimization problem using a gradient-based method, back propagation can be used to calculate the gradient of the function for each iteration.

I.3.3.2 Stochastic Gradient Descent:

Using the convex function in gradient descent algorithms ensures finding an optimal minimum without getting trapped in a local minimum. Depending upon the values of the function and learning rate or step size, it may arrive at the optimum value in different paths and manners.

I.3.3.3 Learning Rate Decay:

Adjusting the learning rate increases the performance and reduces the training time of stochastic gradient descent algorithms. The widely used technique is to reduce the learning rate gradually, in which we can make large changes at the beginning and then reduce the learning rate gradually in the training process.

I.3.3.4 Dropout:

The overstating problem in deep neural networks can addressed using the drop out technique. This method applied by randomly dropping units and their connections during training. Dropout offers an effective regularization method to reduce overstating and improve generalization error. Dropout gives an improved performance on supervised learning tasks in computer vision, computational biology, document classification, speech recognition.

I.3.3.5 Max-Pooling:

In max pooling, a filter is predefined, and this filter then applied across the no overlapping sub-regions of the input taking the max of the values contained in the window as the output. Dimensionality, as well as the computational cost to learn several parameters, can reduced using max pooling.

I.3.3.6 Batch Normalization:

Batch normalization reduces covariate shift, thereby accelerating deep neural network. It normalizes the inputs to a layer, for each mini-batch, when the weights updated during the training.

Normalization stabilizes learning and reduces the training epochs. The stability of a neural network can increased by normalizing the output from the previous activation layer.

I.3.3.7 Skip-gram:

Word embedding algorithms can modeled using Skip-gram. In the skip-gram model, two vocabulary terms share a similar context; then those terms are identical. For example, the sentences cats’’ are mammals” and dogs are mammals” are meaningful sentences which shares the same meaning” are mammals.” Skip-gram can implemented by considering a context win down containing n terms and train the neural network by skipping one of this term and then use the model to predict skipped term.

I.3.3.8 Transfer learning:

In transfer learning, a model trained on a particular task exploited on another related task. The knowledge obtained while solving a particular problem can transferred to another network, which is trained on a related problem. This allows for rapid progress and enhanced performance while solving the second problem.

I.3.4 Deep Learning Platforms:

A deep learning framework helps in modeling a network more rapidly without going into details of underlying algorithms. Each framework built for different purposes differently.

I.3.4.1 Tensor Flow:

Tensor Flow, developed by Google brain, supports languages such as Python, C++and R. It enables us to deploy our deep learning models in CPUs as well as GPUs.

I.3.4.2 Keras:

Keras is an API, written in Python and run on top of Tensor Flow. It enables fast experimentation. It supports both CNNs and RNNs and runs on CPUs and GPUs.

I.3.4.3 PyTorch:

PyTorch can used for building deep neural networks as well as executing tensor computations. PyTorch is a Python-based package that provides Tensor computations. PyTorch delivers a framework to create computational graphs.

I.3.4.4 Caffe:

Yangqing Jia developed Caffe, and it is open source as well. Caffe stands out from other frameworks in its speed of processing as well as learning from images. Caffe Model Zoo framework facilitates us to access pre-trained models, which enable us to solve various problems effortlessly.

I.3.4.5 Deeplearning4j:

Deeplearnig4j implemented in Java, and hence, it is more efficient when compared to Python. The ND4J tensor library used by Deeplearning4j provides the capability to work with multi-dimensional arrays or tensors. This framework supports CPUs and GPUs. Deeplearnig4j works with images, cases well as plaintext. [33]

Table I.1: Deep-Learning Framework Language written in.

Deep-Learning Framework	Release Year	Language written in	CUDA supported	Pre-trained models
Tensor Flow	2015	C++, Python	yes	yes
Keras	2015	Python	yes	yes
PyTorch	2016	Python, C	yes	yes
Caffe	2013	C++	yes	yes
Deeplearning4j	2014	C++, Java	yes	yes

I.3.5 Applications areas for Deep Learning:

I.3.5.1 Virtual Assistants:

Virtual Assistants are cloud-based applications that understand natural language voice commands and complete tasks for the user. Amazon Alexa, Cortana, Siri, and Google Assistant are typical examples of virtual assistants. They need internet-connected devices to work with their full capabilities. Each time a command is fed to the assistant, they tend to provide a better user experience based on past experiences using Deep Learning algorithms.

I.3.5.2 Chatbots:

Chatbots can solve customer problems in seconds. A chatbot is an AI application to chat online via text or text-to-speech. It is capable of communicating and performing actions similar to a human.

Chatbots are used a lot in customer interaction, marketing on social network sites, and instant messaging the client. It delivers automated responses to user inputs. It uses machine learning and deep learning algorithms to generate different types of reactions.

I.3.5.3 Healthcare:

Deep Learning has found its application in the Healthcare sector. Computer-aided disease detection and computer-aided diagnosis have been possible using Deep Learning. It is widely used for medical research, drug discovery, and diagnosis of life-threatening diseases such as cancer and diabetic retinopathy through the process of medical imaging.

I.3.5.4 Entertainment:

Companies such as Netflix, Amazon, YouTube, and Spotify give relevant movies, songs, and video recommendations to enhance their customer experience. This is all thanks to Deep Learning. Based on a person's browsing history, interest, and behavior, online streaming companies give suggestions to help them make product and service choices. Deep learning techniques are also used to add sound to silent movies and generate subtitles automatically.

I.3.5.5 News Aggregation and Fake News Detection:

Deep Learning allows you to customize news depending on the readers' persona. You can aggregate and filter out news information as per social, geographical, and economic parameters and the individual preferences of a reader. Neural Networks help develop classifiers that can detect fake and biased news and remove it from your feed. They also warn you of possible privacy breaches.

I.3.5.6 Image Captioning:

Image Captioning is the method of generating a textual description of an image. It uses computer vision to understand the image's content and a language model to turn the understanding of the image into words in the right order. A recurrent neural network such as an LSTM used to turn the labels into a coherent sentence. Microsoft has built its caption bot where you can upload an image or the URL of any image, and it will display the textual description of the image. Another such application that suggests a perfect caption and best hashtags for a picture is Caption AI [38].

I.3.6 The neural network

Neural network is a system modeled on the human brain, consisting of an input layer, multiple hidden layers, and an output layer. Data fed as input to the neurons. The information transferred to the next layer using appropriate weights and biases. The output is the final value predicted by the artificial neuron [36]. She is work on algorithms, which pass data between each other as it is processed. Such neural networks form a part of deep learning technologies [37].

I.3.6.1 the Human Brain and the Neural Network:

The human brain receives and transmits information via nerve cells (neurons). The human brain consists of many billions of neurons to form an elaborate network like structure. It is estimated that an average human brain consists of 86 billion neurons. The neurons in this dense network work in collaboration to ensure that the information needed to be passed on to the desired place, such as the muscle in your heart, is completed with the maximum speed and accuracy in order to allow your heart to pump at a particular rate depending on how much blood your body needs to be circulating at any one time.

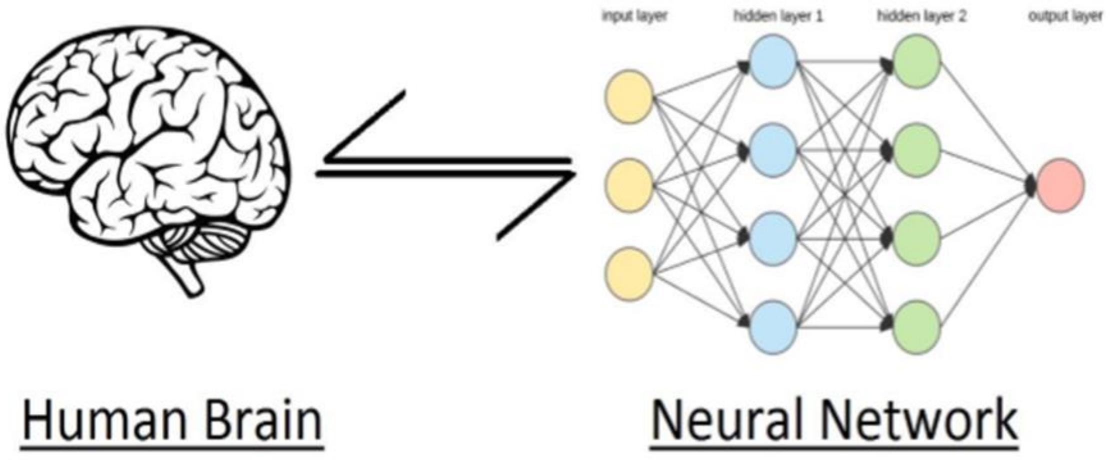


Figure I.9: Similarities between a human brain and neural network.

A neuron consists of three distinct parts: a cell body, a dendrite, and an axon. The cell body is the largest part of a neuron and consists of the nucleus and cytoplasm. Dendrites are extensions that are responsible for receiving messages from other neurons, and the axon is that part of a neuron that is responsible for sending the signals. These nerve cells pass on the information as electrical impulses to the adjacent cells via the synapse.

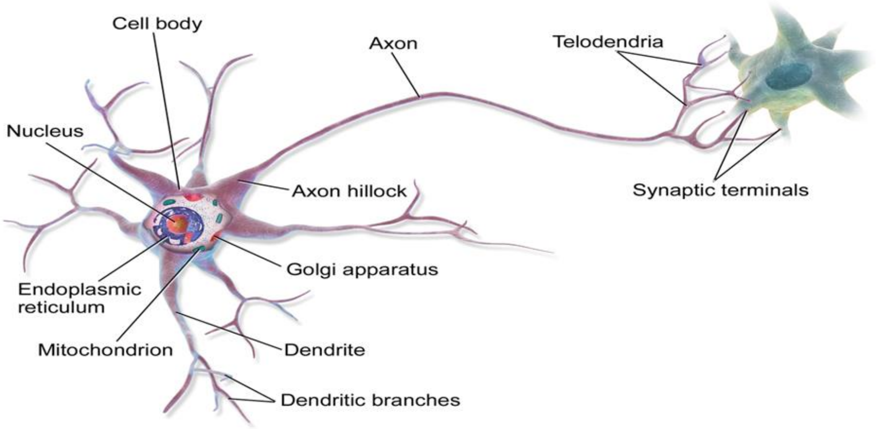


Figure I.10: A neuron of the human brain.

A similar concept is adopted for algorithms in machine learning. The 'neurons' in the neural network are artificially created in a computer and joined to other such 'neurons' present in the network. This creates the neural network. The artificial neuron imitates the working of a biological neuron.[37]

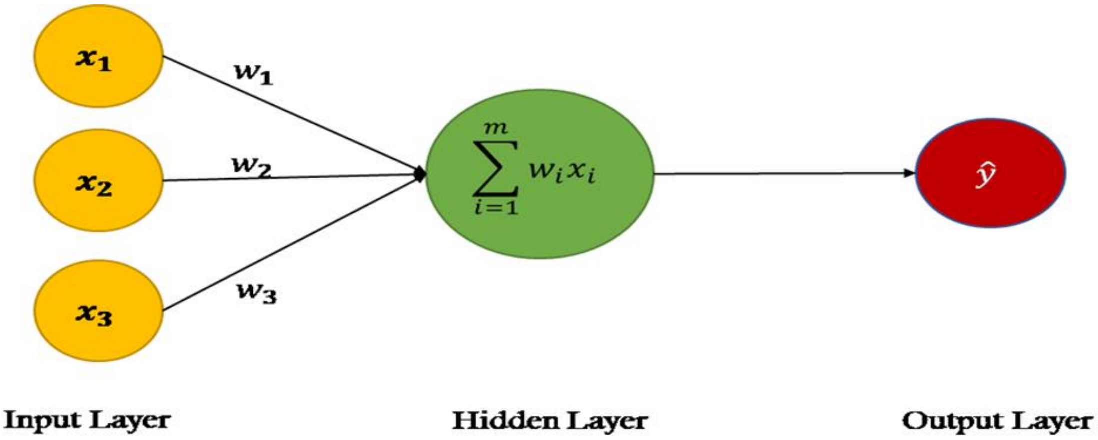


Figure I.11: Artificial neuron of the neural network.

I.3.7 Types of Activation Functions:

Net inputs are the most important units in the structure of a neural network which are processed and changed into an output result known as unit's activation by applying function called the activation function or threshold function or transfer function which is a a scalar to scalar transformation.

To enable a limited amplitude of the output of a neuron and enabling it in a limited range known as squashing functions. A squashing function squashes the amplitude of output signal into a finite value.

I.3.7.1 Sigmoid Activation Function:

It is the most widely used activation function as it is a non-linear function. Sigmoid function transforms the values in the range 0 to 1. It can be defined as: f(x) = 1/e-x

Sigmoid function is continuously differentiable and a smooth S-shaped function. The derivative of the function: f'(x) = 1-sigmoid(x)

Also sigmoid function is not symmetric about zero which means that the signs of all output values of neurons will be same. This issue can improved by scaling the sigmoid function.

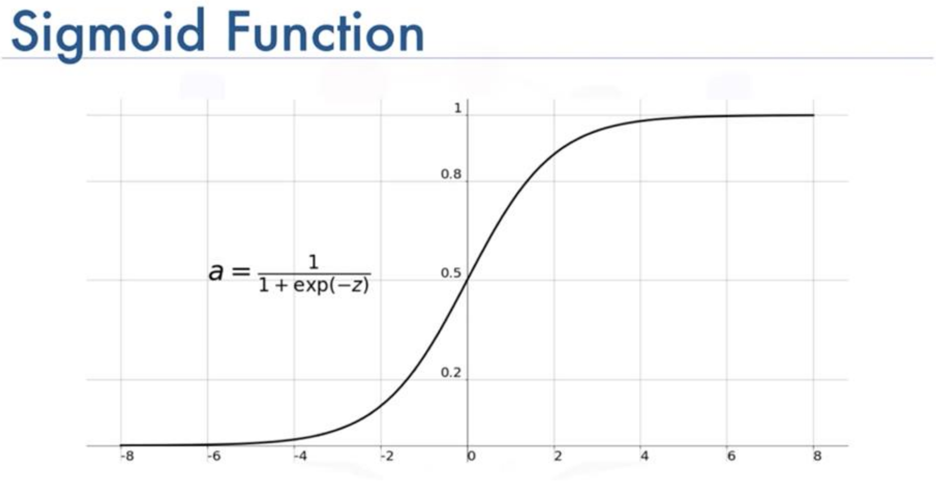


Figure I.12: Sigmoid Activation Function.

I.3.7.2 Relu Activation Function:

Relu stands for rectified liner unit and is a non-linear activation function which widely used in neural network. The upper hand of using Relu function is that not all the neurons are activated at the same time; this implies that a neuron will be deactivated only when the output of linear transformation is zero. It can be defined mathematically as: f(x) = max(0,x)

Relu is more efficient than other functions because as all the neurons are not activated at the same time, rather a certain number of neurons are activated at a time. In some cases, the value of gradient is neural network zero, due to which the weights and biases are not updated during back propagation step in training.

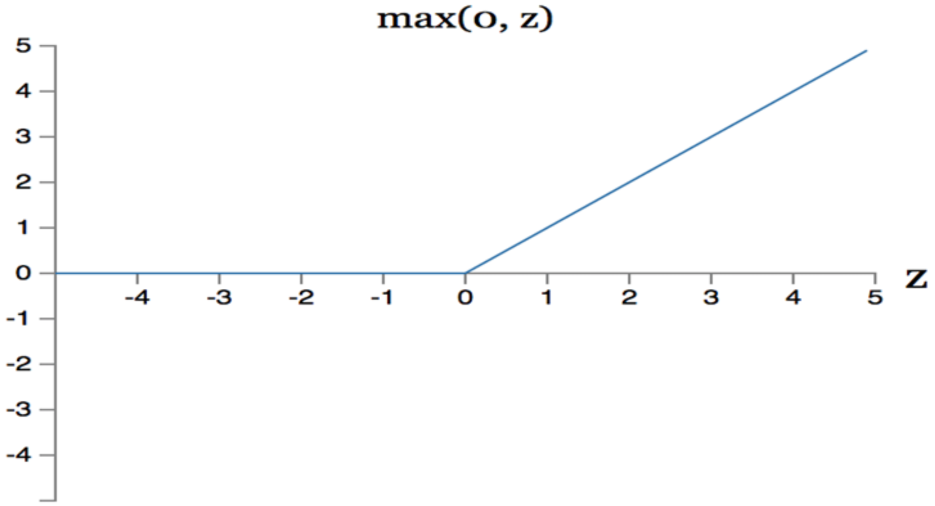


Figure I.13: ReLu Activation Function plot.

I.3.7.3 Softmax Activation Function:

Softmax function is a combination of multiple sigmoid functions. As we know that a sigmoid function returns values in the range 0 to 1, these can treated as probabilities of a particular class' data points. Softmax function unlike sigmoid functions, which used for binary classification, can used for multiclass classification problems. The function, for every data point of all the individual classes, returns the probability. It can expressed as:

$$\sigma(z)_j = \frac{e_j^z}{\sum_{k=1}^{K} ez_k} \text{ For j=1,…., K.}$$

When we build a network or model for multiple class classification, then the output layer of the network will have the same number of neurons as the number of classes in the targe. [39]

I.3.8 Types of Deep Neural Networks (DNN):

I.3.8.1 Single Layer Perceptron Model (SLP):

The single layer perceptron (SLP) model is the simplest form of neural network and the basis for the more advanced models that have been developed in deep learning. Typically, we use SLP in classification problems where we need to give the data observations labels (binary or multinomial) based on inputs. The values in the input layer directly sent to the output layer after they multiplied by weights and a bias added to the cumulative sum. This cumulative sum then put into an activation function, which is simply a function that defines the output. When that output is above or below a user-determined threshold, the final output is determined. Researchers McCulloch-Pitts Neurons described a similar model in the 1940s.

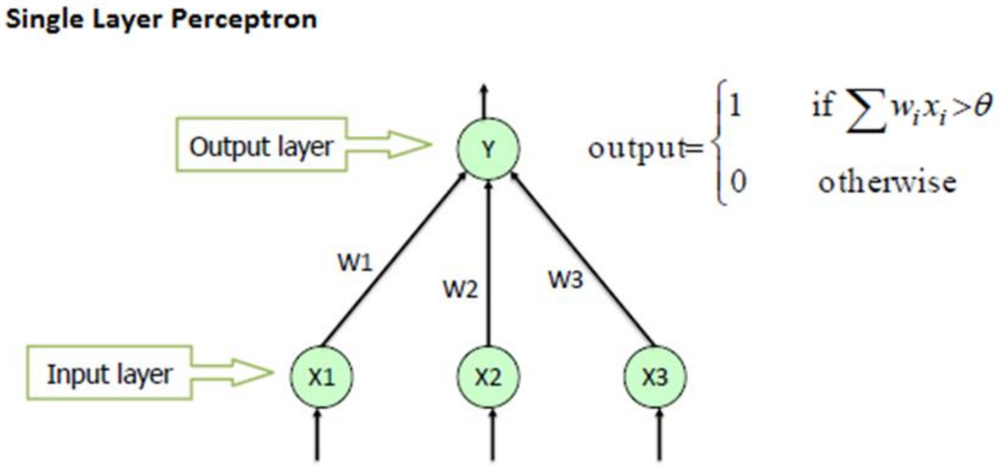

Single Layer Perceptron
Output layer
Y
$\text{output} = \begin{cases} 1 & \text{if } \sum w_i x_i > \theta \\ 0 & \text{otherwise} \end{cases}$
W1
W2
W3
Input layer
X1
X2
X3

Figure I.14: Single Layer Perceptron Model.

I.3.8.2 Multilayer Perceptron Model (MLP):

Very similar to SLP, the multilayer perceptron (MLP) model features multiple layers that are inter connected in such a way that they form a feed-forward neural network. Each neuron in one layer has directed connections to the neurons of a separate layer. One of the key distinguishing factors in this model and the single layer perceptron model is the back-propagation algorithm, a common method of training neural networks. Back-propagation passes the error calculated from the output layer to the input layer such that we can see each layer’s contribution to the error and alter the network accordingly. Here, we use a gradient descent algorithm to determine the degree to which the weights should change upon each iteration. Gradient descent—another popular machine learning/optimization algorithm—is simply the derivative of a function such that we find a scalar (a number with magnitude as its only property) value that points in the direction of greatest momentum. By subtracting the gradient, this leads us to a solution that is more optimal than the one we currently are at until we reach a global optimum.

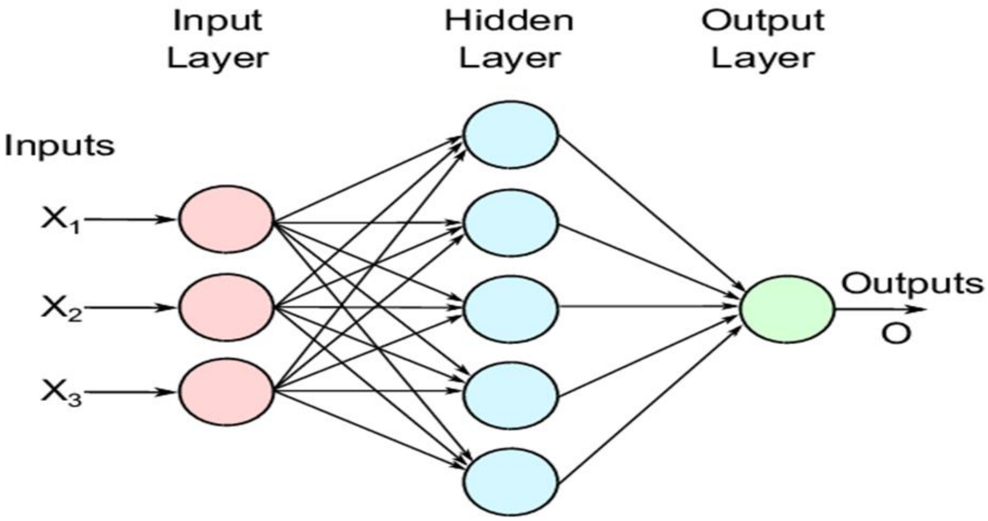


Figure I.15: Multilayer Perceptron Model.

I.3.8.3 Convolutional Neural Networks (CNNs):

Convolutional neural networks (CNNs) are models that most frequently used for image processing and computer vision. They designed in such a way to mimic the structure of the animal visual cortex. Specifically, CNNs have neurons arranged in three dimensions: width, height, and depth. The neurons in a given layer only connected to a small region of the prior layer. CNN models most frequently used for image processing and computer vision.

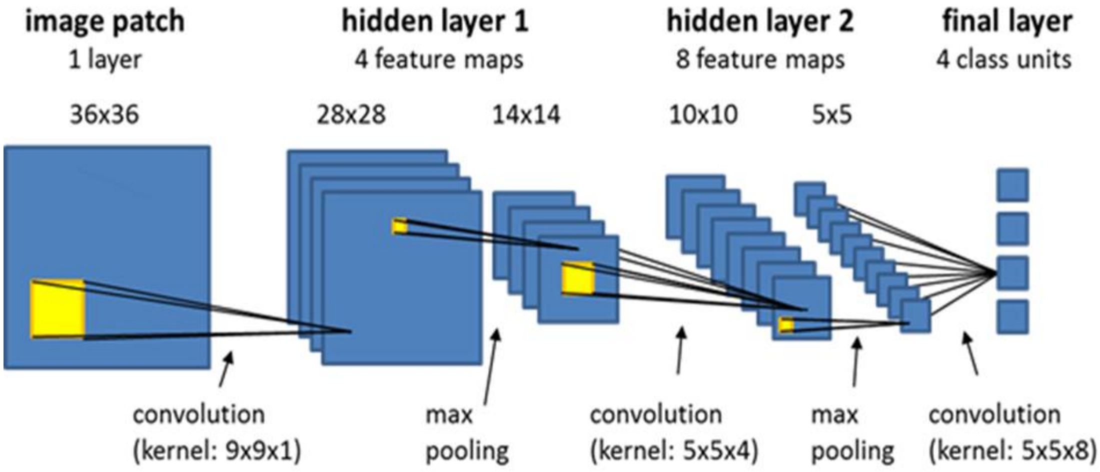


Figure I.16: Convolutional neural networks.

I.3.8.4 Recurrent Neural Networks (RNNs):

Recurrent neural networks (RNNs) are models of artificial neural networks (ANNs) where the connections between units form a directed cycle. Specifically, a directed cycle is a sequence where the walk along the vertices and edges completely determined by the set of edges used and therefore has some semblance of a specific order. RNNs often specifically used for speech and handwriting recognition.

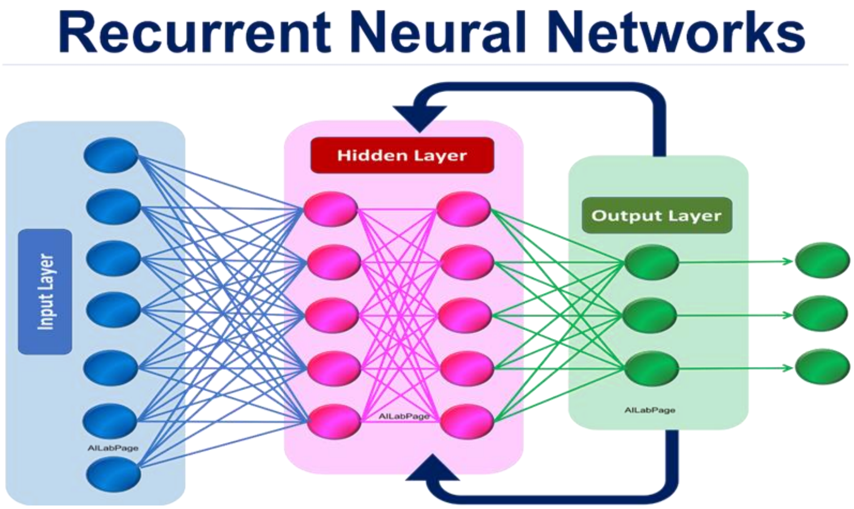


Figure I.17: Recurrent Neural Networks

I.3.8.5 Restricted Boltzmann Machines (RBMs):

Restricted Boltzmann machines are a type of binary Markov model that have a unique architecture, such that there are multiple layers of hidden random variables and a network of symmetrically coupled stochastic binary units. DBMs are comprised of a set of visible units and series of layers of hidden units. There are, however, no connections between units of the same layer. DMBs can learn complex and abstract internal representations in tasks such as object or speech recognition.

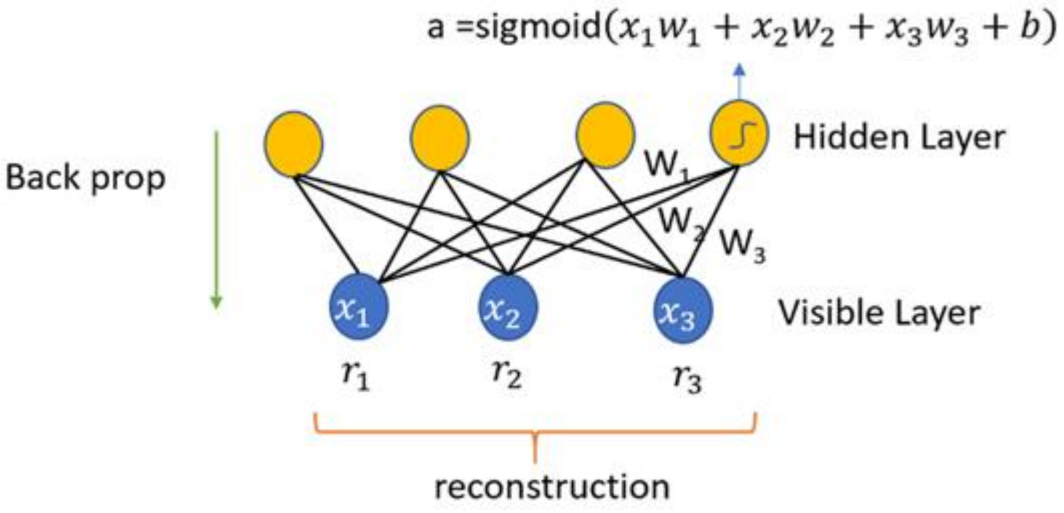


Figure I.18: Restricted Boltzmann Machines.

I.3.8.6 Deep Belief Networks (DBNs):

Deep belief networks are similar to RBMs except each sub network is hidden layer is in fact the visible layer for the next sub network. DBNs are broadly a generative graphical model composed of multiple layers of latent variables with connections between the layers but not between the units of each individual layer. [33]

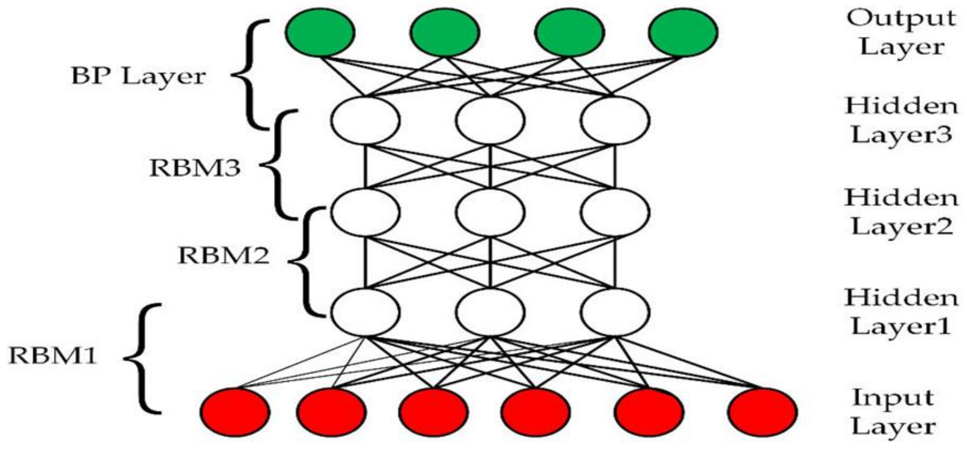


Figure I.19: Deep Belief Networks.

I.3.9 Comparison between Machine Learning and Deep Learning:

Machine Learning is a set of algorithms that have the capability to analyze the data provided, learn from that data, and apply what learnt to make intelligent decisions. Many prominent examples can found on social media, and photo storage platforms, which capable of identifying people from unloaded images, or recommending movie and television program based on what you have watched via a streaming app. This learning based on the past actions, selections and preferences of the user. Machine learning may need human intervention at times and tend to perform limited tasks for what they have been programmed as it does not think beyond the realms of what it has been programmed for and subsequently learnt to do within those realms.

Deep learning contains a complex hierarchy of concepts, each one defined and related to the other in some form of the other. The development of a deep learning technique involves the processing of the data through various layers through a step-by-step process. Among the various benefits of using deep learning techniques, the two most prominent ones are:

- Scalability - ability of a computing process used across a range of applications.

- Feature Learning - ability to perform automatic feature extraction from raw data

Deep learning machines tend to require enormous amounts of data as well as high-end computers to generate the desired results. A graphics processing unit, or GPU, is also an integral part of a deep learning system in order to process images in parallel with computations on data.

Whilst both machine learning and Deep Learning are subsets of AI, their approaches to solving a problem are completely different from each other. Let us see how. Here is an image containing a mixture of cats and dogs.

Figure I.20: A collective image of dogs and cats.

The algorithm which machine learning uses labeled, or structured data, which contains all the properties of the animals in order for it to be able to identify the individual figures in the image. However, the approach of the deep learning algorithm is slightly different. The algorithm will still be able to identify the individual figures in the image using various hidden layers in the algorithm. These layers contain the key to the properties of the animals to the image and thus can deal or respond to the unsupervised data.[37]

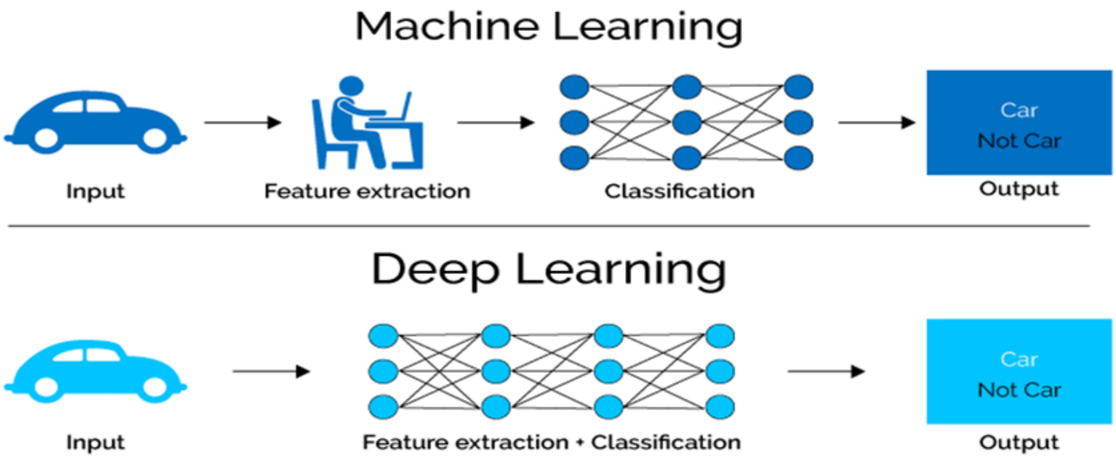


Figure I.22: Comparison between Machine Learning and Deep Learning.

I.4 Conclusion:

In this chapter we have presented the important notions that are related to machine and deep learning (definition, Architectures, etc.). Deep learning contains a complex hierarchy of concepts, each one defined and related to the other in some form of the other. The development of a deep learning technique involves the processing of the data through various layers through a step-by-step process.

.

Chapter II

Wireless Network Security

Chapter II: Wireless Network Security

II.1 Introduction:

Recently, the enormous development in technology has led to the expansion of networks and the increase in their number and size dramatically, which led to a mismatch between the networks, which became difficult to establish communication between them based on different specifications and standards. To solve this problem, the Organization for Standardization examined the structures of the networks. It would help designers implement networks capable of communicating with each other.

In light of this technological development, wireless networks have become an emerging technology that allows its users to access information and electronic services despite their geographical locations. The success of this type of network has aroused great interest for individuals and industrial environments. It seen as a complementary alternative to traditional wireless networks because it is widely used in local networks. For companies, for purely professional use, personal home local area networks, medium and wide coverage networks as well. Therefore, wireless networks are dominant in the current era.

In this chapter, different kinds of wireless networks will present Personal Area Networks (WPAN), Local Area Networks (WLAN), Urban Area Networks (WMAN), and Wide Area Networks (WWAN). We will discuss the technologies available in each network, mentioning the advantages and disadvantages of wireless networks.

Then we will study the security of wireless networks and what access protocols we will adopt: FDMA, TDMA, and CDMA.

II.2 wireless network:

II.2.1 Definition:

A wireless network is a set of devices connected to each other and which can send each other and receive data without any physical “wired” link connecting, these different components between them is necessary. [1]

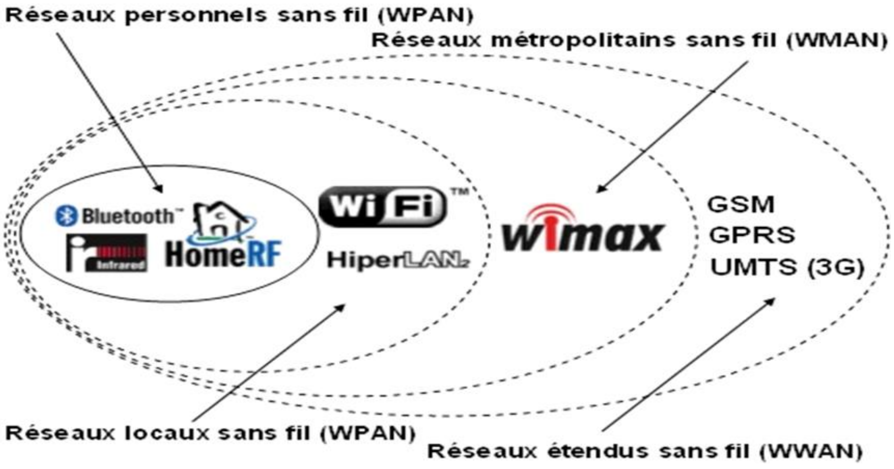

Réseaux personnels sans fil (WPAN)
Réseaux métropolitains sans fil (WMAN)
Bluetooth
Infrared
HomeRF
WiFi
HiperLAN2
wimax
GSM
GPRS
UMTS (3G)
Réseaux locaux sans fil (WPAN)
Réseaux étendus sans fil (WWAN)

Figure II.1: classification of wireless networks.

II.2.2 Type of Wireless network:

II.2.2.1 Wireless Personal Area Networks (WPAN):

The personal wireless network (also called individual wireless network or network wireless home automation and rated WPAN for Wireless Personal Area Network) concerns short-range wireless networks: of the order of a few tens of meters [2].

This type of network generally used to connect peripherals (printer, telephone laptop, household devices ...) or a personal assistant (PDA) to a computer without wired link or to allow the wireless link between two very close machines.

There are several technologies used for WPANs:

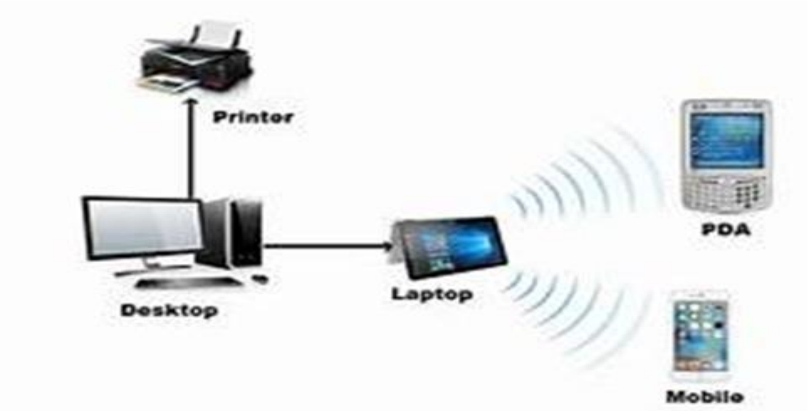


Figure II .2: Example of a WPAN configuration.

II.2.2.1.1 Bluetooth:

Launched by Ericsson in 1994, offering a theoretical speed of 1 Mbps for a range maximum of about thirty meters.

Bluetooth, also known as IEEE 802.15.1, has the advantage of being very low energy intensive, which makes it particularly suitable for use in small peripheral devices. Version 1.2 notably reduces interference with Wi-Fi networks. [2]

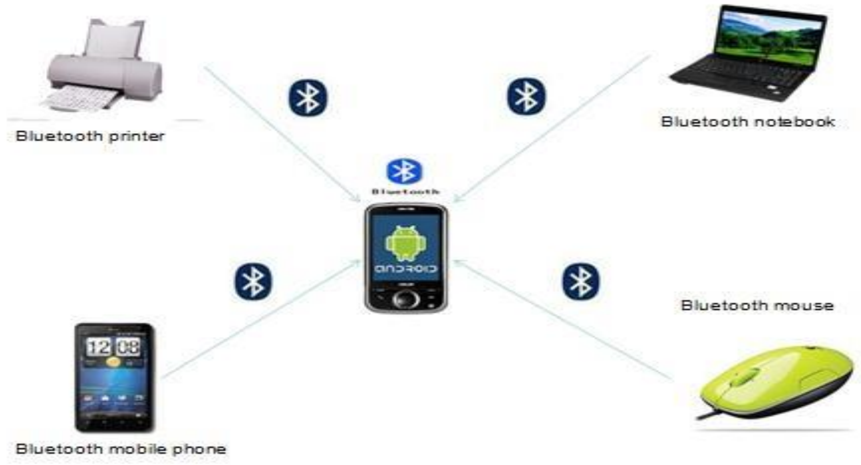


Figure II.3: Bluetooth application areas.

II.2.2.1.2 Home RF :(Home Radio Frequency):

Launched in 1998 by the Home RF working group (formed in particular by the manufactures Compaq, HP, Intel, Siemens, Motorola and Microsoft) offers a theoretical throughput of 10Mbps with a range of approximately 50 to 100 meters without an amplifier.

The Home RF standard supported in particular by Intel was abandoned in January 2003, in particular because the founders of processors are now relying on on-board Wi-Fi technologies (via the technology Centurion, embedding a microprocessor and a Wi-Fi adapter in a single component). [2]

Figure II.4: home RF.

II.2.2.1.3 ZigBee technology: (also known as IEEE 802.15.4):

Provides wireless connections at very low cost and with very low energy consumption, which makes it particularly suitable for being directly integrated in small electronic devices (domestic appliances, stereo, toys, etc.). [2]

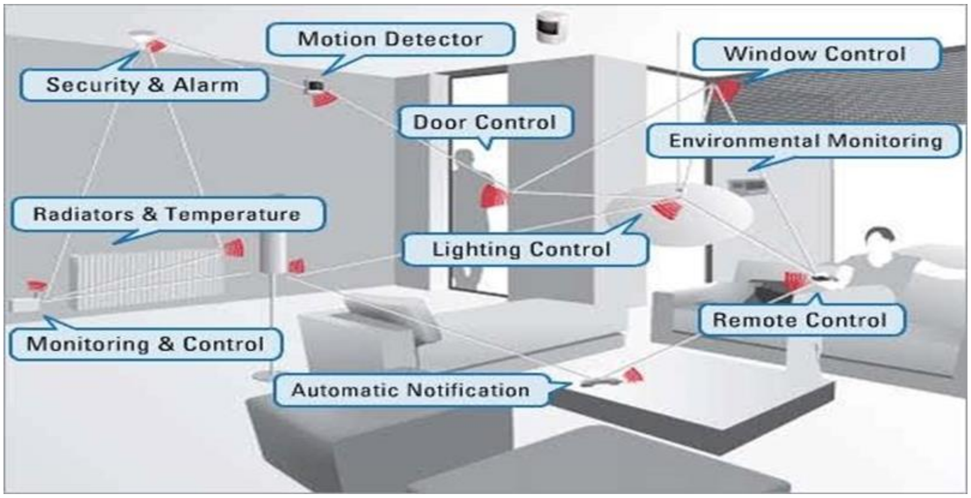


Figure II.5: General information about ZigBee.

II.2.2.1.4 Infrared links

Allow the creation of wireless links of a few meters with speeds up to go up to a few megabits per second. This technology is widely used for home automation (remote controls) but nevertheless suffers from disturbances due to interference bright. The association IrDA (infrared data association) formed in 1995 brings together more than 150 members [2].

Figure II.6: Example of infrared.

II.2.2.2 Wireless Local Area Networks (WLANs):

Wireless Local Area Network (WLAN) is a network to cover the equivalent of a local corporate network, i.e. a range of approximately one hundred meters. It makes it possible to link together the terminals present in the zone of cover.

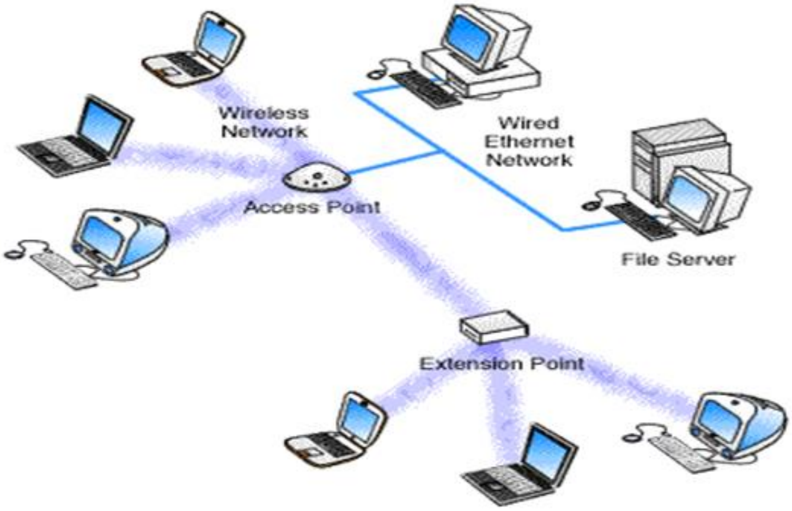


Figure II.7: How WLAN works

There are several competing technologies: Wi-Fi, hiperLAN2 (High Performance Radio LAN 2.0) [2].

II.2.2.2.1 Wi-Fi:

Wi-Fi is a set of wireless communication protocols governed by standards of the IEEE 802.11 group. Thanks to Wi-Fi standards, it is possible to create local networks wireless broadband. In practice Wi-Fi makes it possible to connect laptops, office machines, personal assistants (PDA Personal Digital Assistant), objects communicating or even peripherals to a broadband link from 11 Mbit/s theoretical or 6 Mbit/s real in 802.11b to 54 Mbit/s theoretical or about 25 Mbit/s real in 802.11a or 802.11g over a radius of several tens meters indoors (generally between a twenty and fifty meters).

II.2.2.2.2 HiperLAN2: (High Performance Radio LAN 2.0):

European standard developed by ETSI (European Telecommunications Standards Institute) makes it possible to obtain a theoretical throughput of 54 Mbps over an area of around one hundred meters in the frequency range between 5150 and 5300 MHz [2].

II.2.2.3 Metropolitan wireless networks (WMAN):

The Wireless Metropolitan Area Network (WMAN) known as Local Radio Loop (BLR). WMANs based on the IEEE standard 802.16. The radio local loop offers a useful throughput of 1 to 10 Mbit/s for a range of 4 to 10 kilometers, which primarily targets this technology for operators of Telecommunications, The MAN made up of several LANs of the same company connected between them.

The MAN generally used in universities, campuses or in cities. The physical interconnect medium used in WMAN is usually optical fiber [3].

II.2.2.3.1 Wimax:

Also known IEEE 802.16, Wimax is a standard for high-speed wireless transmission. Operating at 70 Mbit/s, it designed to connect the Wi-Fi access points to a fiber optic network, or to relay a shared connection to broadband to multiple users. With a theoretical range of 50 km, it should allow, in the long term, the development of metropolitan networks (WMAN) based on a single point of access, unlike an architecture based on many access points Wi-Fi [4].

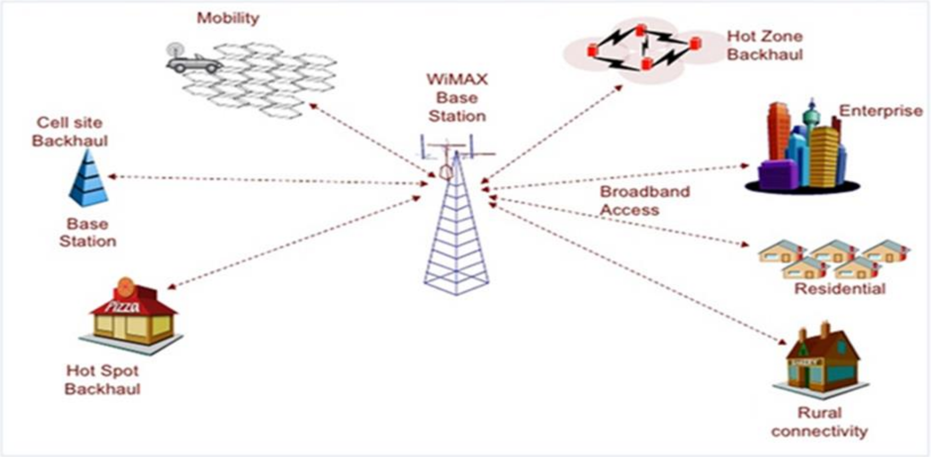


Figure II .8: Principle of operation of Wimax.

II.2.2.4 Wireless Wide Area Networks (WWAN):

The Wireless Wide Area Network (WWAN) also known as the mobile cellular network. These are the most common wireless networks since all mobile phones connected to a wide area wireless network. The main technologies are as follows:

- GSM (Global System for Mobile Communication or Special Mobile Group).
- GPRS (General Packet Radio Service).
- UMTS (Universal Mobile Telecommunication System).

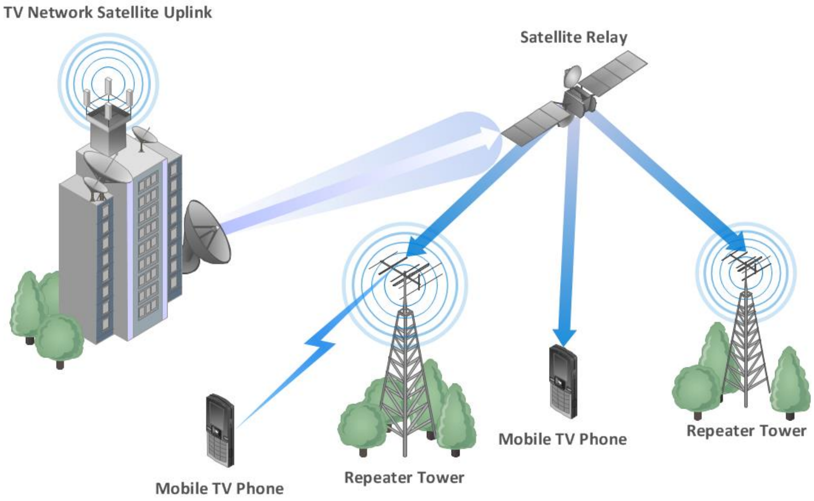


Figure II.9: WWAN network.

II.2.2.4.1 GSM:

GSM is a digital cellular radiotelephone system, which offers its subscribers of services that enable end-to-end mobile station communication to through the network. Telephony is the most important service offered. This network allows communication between two mobile stations or between a mobile station and a fixed station. Other services offered are data transmission and message transmission short alphanumeric. [5]

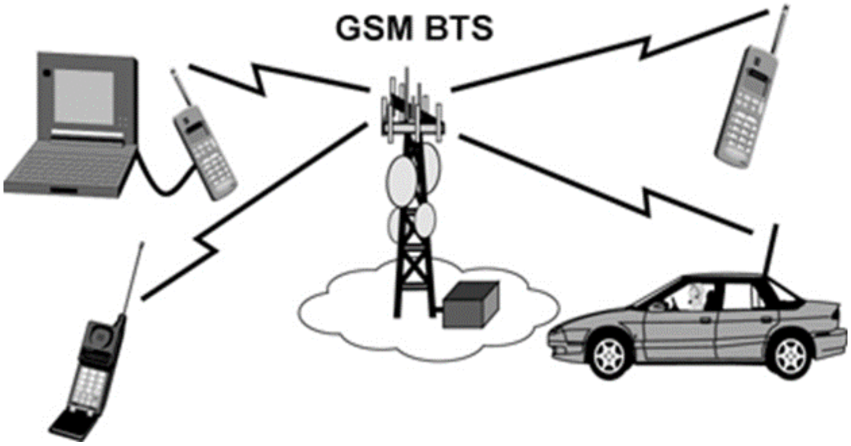


Figure II.10: Architecture of the GSM network.

II.2.2.4.2 GPRS:

The General Packet Radio Service or GPRS is a standard (network protocol) for mobile telephony derived from GSM and complementary to it, allowing a higher data rate. It often referred to as 2.5G or 2G+. The G is the abbreviation for generation and the 2.5 indicates that it is a technology halfway between GSM (second generation) and UMTS (third generation).

GPRS is an extension of the GSM protocol: it adds packet transmission to the latter. This method is more suitable for data transmission. Indeed, the resources allocated only when data exchanged, contrary to the “circuit” mode in GSM where a circuit is established – and the associated resources – for the entire duration of the communication. GPRS then evolved in the early 2000s to the Edge standard, which also optimized for transferring data and which uses the same antennas and the same radio frequencies. [6]

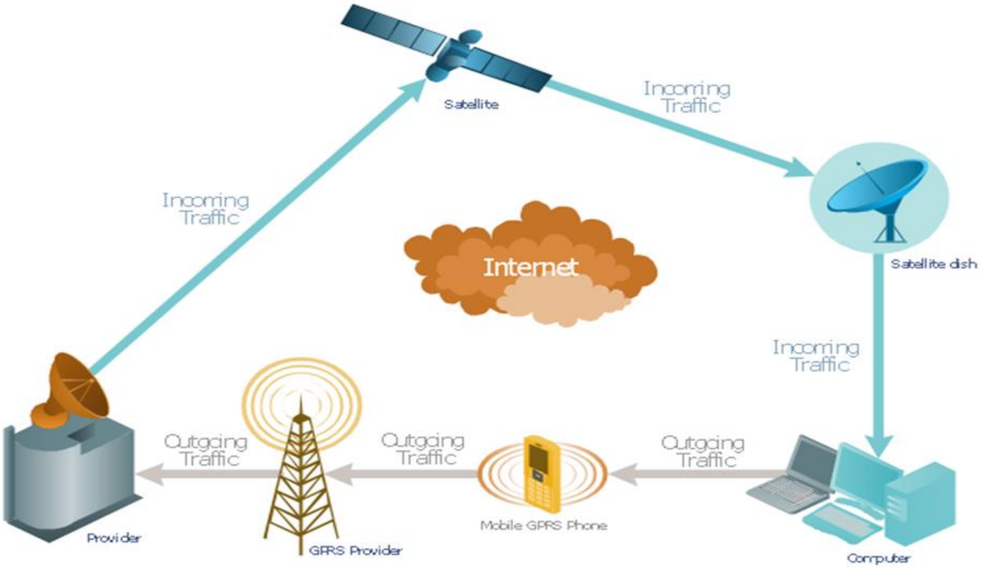


Figure II.11: GPRS application areas.

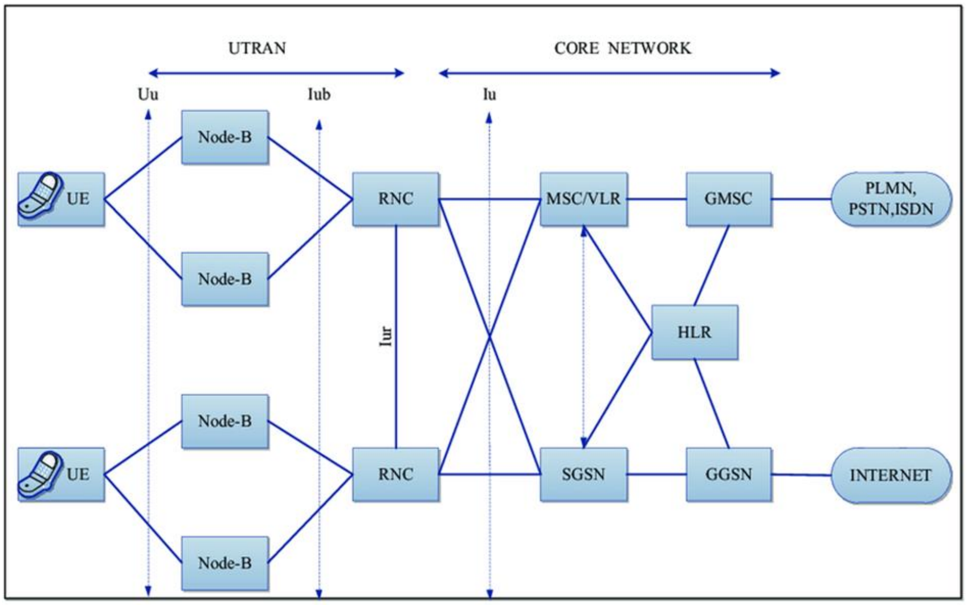
II.2.2.4.3 L'UMTS:

The Universal Mobil Telecommunication System (UMTS) is the new mobile telephony standard, also more generally called third generation telephony or 3G. The term W-CDMA (Wideband Code Division Multiple Access), is more often used, which takes the name of the technology deployed in Europe and by certain Asian operators.

UMTS is the 3rd generation mobile network system, after GSM qualified as the 2nd generation mobile network.

The techniques used will make it possible to reach speeds of 384 Kbit/s and even 2 Mbit/s. UMTS networks will be used for data transfer, for multimedia, and voice.

Two types of radio access provided. Access via terrestrial network (such as GSM) and direct access via satellite link. [7]



.**Figure II.12:** Architecture of UMTS.

II.2.3 Advantages and disadvantages of wireless networks:

Table II.1: Advantages and disadvantages of wireless networks.

Advantages are	Disadvantages are
✓ Mobility(easy).	✓ Mobility(insecure).
✓ Cost-effective in the initial phase.	✓ High cost post-implementation.
✓ Easy connection.	✓ No physical protection of networks.
✓ Different ways to transmit data.	✓ Hacking has become more convenient.
✓ Easy sharing.	✓ Risk of data sharing is high.

II.2.4 Wireless network applications:

- Industrial process and control applications where wired connections are too costly or inconvenient, e.g., continuously moving machinery.
- Emergency applications that require immediate and transitory setup, such as battlefield or disaster situations.
- Mobile applications, such as asset tracking.
- Surveillance cameras (maybe you do not want those easily noticed, cables difficult to hide).
- Vertical markets like medical, education, and manufacturing.

- Communication with other Wi-Fi devices, like a laptop or a PDA.
- Machine to Machine (M2M) applications.[8]

II.3 security:

Wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which connected by a network cable. However, wireless networks broadcast data in every direction to every device that happens to be listening, within a limited range. A wired network can secured at its edges, for example, by restricting physical access and installing firewalls. A wireless network with the same measures in place is still vulnerable to eavesdropping. Therefore, wireless networks require a more focused effort to maintain security. [8]

II.3.1 Types of Wireless Security:

II.3.1.1 WEP:

WEP (Wired Equivalent Privacy) is an old encryption type. It used extensively in wireless networking even though it is quite easy to hack in to. It is the default encryption on many wireless routers and as a result it is currently the most commonly used. Use this if you are not too worried about a geek hacking in and stealing your internet connection. The chances are small. Otherwise, go for something better.

II.3.1.2 WPA:

WPA (Wi-Fi Protected Access) addresses the shortcomings of WEP and is much far more difficult to hack. WPA came out around 2002. The geek next door may take 10 minutes to hack your WEP, but may take a day or two to hack WPA. WPA was the interim format while WPA2 is the final, more secure, version.

II.3.1.3 WPA-TKIP:

Security type WPA and the encryption type TKIP. TKIP (Temporary Key Integrity Protocol) used within WPA above. This solution is very hard to hack but there is a flaw in the encryption, which presents a slight vulnerability. The great thing about TKIP is it is compatible with older hardware (pre 2003 wireless network cards).

II.3.1.4 WPA-AES:

Advanced Encryption Standard, AES is not compatible with pre 2003 hardware but is almost impossible to hack if a good key/passphrase chosen. The US government as their standard encryption has adopted AES. It is the used in the final version of WPA (WPA2).

II.3.1.5 WPA-PSK:

Pre Shared Key. All of the above use PSK (Pre Shared Key). Which just means you have chosen a passphrase or key that will know by the router and the computer to connect each other [9]

The comparison of WEP, WPA, and WPA2 can summarized in the following table:

Table II.2: The difference between WEP, WPA and WPA2.

	WEP	**WPA**	**WPA2**
Encryption	RC4	RC4	AES
Key rotation	NONE	Dynamic session keys	Dynamic session keys
Key distribution	Manually typed into each device	Automatic distribution available	Automatic distribution available
Authentication	Uses WEP key as authentication	Can use 802.1X EAP supported	Can use 802.1X EAP supported

II.3.2 Wireless Network Attacks:

II.3.2.1 Accidental Association:

Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company’s

Overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop hooked to a wired network.

II.3.2.2 Malicious Association:

"Malicious associations" are when wireless devices can actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops known as "soft APs" and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point.

II.3.2.3 Ad-hoc networks:

Ad-hoc networks can pose a security threat. Ad-hoc networks defined as peer-to peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can used to provide security.

II.3.2.4 Non-traditional networks:

Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should secured. IT personnel who have narrowly focused on laptops and access points can easily overlook these nontraditional networks.

II.3.2.5 Identity theft (MAC spoofing):

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering only allow authorized computers with specific MAC IDs to gain access and utilize the network.

II.3.2.6 Man-in-the-middle attacks:

A man-in-the-middle attacker entices computers to log into a computer, which is set up as a soft AP (Access Point). Once this done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. Man-in-the-middle attacks enhanced by software such as LAN jack and Air Jack, which automate multiple steps of the process.

II.3.2.7 Denial of service:

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

II.3.2.8 Network injection:

In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

II.3.2.9 Caffe Latte attack:

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes. [8]

II.3.3 Securing Wireless Transmissions:

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

II.3.3.1 Protecting the Confidentiality of Wireless Transmissions:

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal intercepted.

II.3.3.1.1 Signal-Hiding Techniques:

In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning off the service set identifier (SSID) broadcasting by wireless access points, Assign cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage or Locating wireless access points in the interior of the building, away from windows and exterior walls.

II.3.3.1.2 Encryption:

The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

II.3.3.2 Preventing Alteration of Intercepted Communications:

Interception and alteration of wireless transmissions represents a form of "man-intermeddle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

II3.3.3 Countermeasures to Reduce the Risk of Denial-of-Service Attacks:

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area. [8]

II.3.4 Securing Wireless Access Points:

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:

- Eliminating rogue access points.
- Properly configuring all authorized access points.
- Using 802.1 xs to authenticate all devices.

II.3.4.1 Eliminate Rogue Access Points:

The best method for dealing with the threat of rogue access points is to use 802.1 xs on the wired network to authenticate all devices that are plugged into the network. Using 802.1 xs will prevent any unauthorized devices from connecting to the network.

II.3.4.2 Secure Configuration of Authorized Access Points:

Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

II.3.4.3 Use 802.1x to authenticate all Devices

Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

II.3.5 Securing Wireless Client Devices:

Two major threats to wireless client devices are (1) loss or theft, and (2) compromise. Loss or theft of laptops and PDAs is a serious problem. Laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties.

II.3.6 Securing Wireless Networks:

II.3.6.1 Use of Encryption:

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn’t have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on.

II.3.6.2 Use anti-virus and anti-spyware software, and a firewall:

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

II.3.6.3 Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

II.3.6.4 Change the identifier on the router from the default:

The identifier for the router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if the router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access the network. Changing the identifier to something only you know, and remember to configure the same unique ID into the wireless router and computer so they can communicate.

II.3.6.5 Change your router pre-set password for administration:

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

II.3.6.6 Allow only specific computers to access your wireless network:

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses access to the network.

II.3.6.7 turning off the wireless network when it is not used:

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

II.3.6.8 The Public “hot spots” not always secured:

Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers’ use. [8]

II.4 Multiplex method:

In our environment, we continuously exchange information using the air interface. In the case of mobile telephony, the air interface called "Um". The three main methods used to share the same interface: frequency, time or code. The first method used by the analog systems is the frequency division FDMA (Frequency Division Multiple Access) thereafter, with the digital systems appears the division in time TDMA (Time Division Multiple Access). The last system is CDMA spread spectrum distribution (Code Division Multiple Access) where a code allows access to our unique interface to be distributed. [10]

II.4.1. FDMA (Frequency Division Multiple Accesses):

The FDMA technique was the first method to be developed and used in analog telephone systems. For this type of multiple accesses, a frequency band is allocated to each user. The entire juxtaposed are transmitted on the same transmission channel. In reception, a selective filter tuned to the frequency band of the desired user makes it possible to recover the data. [10]

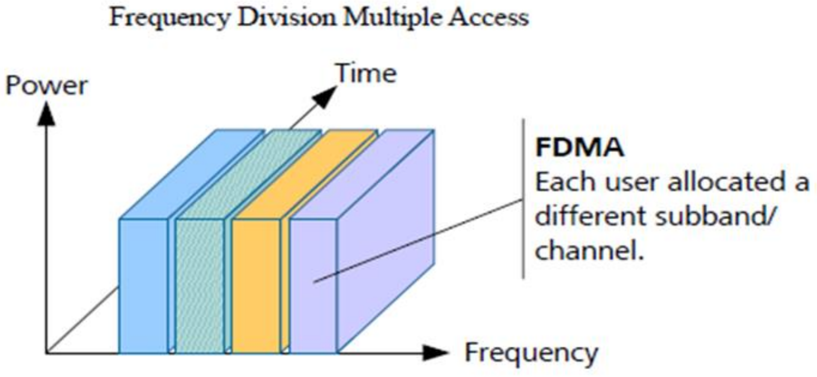

Frequency Division Multiple Access
Power
Time
FDMA
Each user allocated a different subband/ channel.
Frequency

Figure II.13: The FDMA multiple access technique.

II.4.2. TDMA (Time Division Multiple Accesses):

The TDMA method is based on the distribution of time resources. The users share the same bandwidth and transmit the data to be transmitted in the different time intervals or "slot" allocated to them. The receiver performs the demultiplexing operation to recover the data. [10]

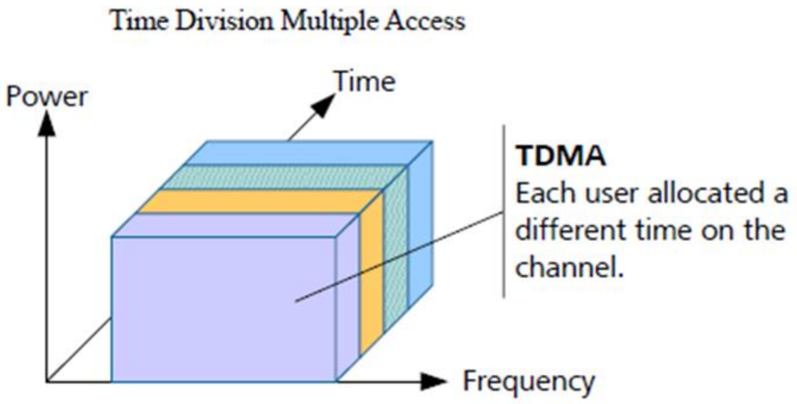

Time Division Multiple Access
Power
Time
TDMA
Each user allocated a different time on the channel.
Frequency

Figure II.14: The TDMA multiple access technique.

II.4.3. CDMA (Code Division Multiple Accesses):

With the CDMA method, all users have simultaneous access to the entire band; they are distinguished on reception thanks to distinct codes for each of them, on a single medium synchronously or asynchronously. [10]

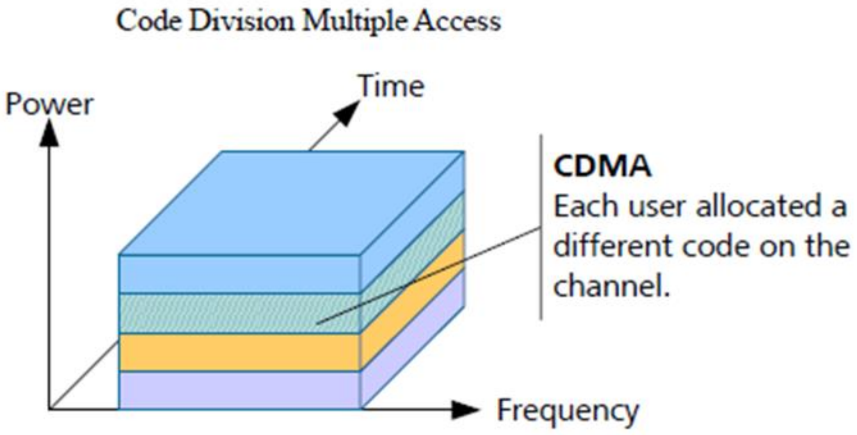

Code Division Multiple Access
Power
Time
CDMA
Each user allocated a different code on the channel.
Frequency

Figure II.15: the CDMA multiple access technique.

There are two main varieties of CDMA:

- FH-CDMA (Frequency Hop) this system resembles a frequency multiplexing in which the allocation of frequencies would vary rapidly (compared to the speed information to transmit).
- DS-CDMA (Direct Sequence) it is to this type of CDMA that we generally do reference when talking about CDMA.

II.4.3.1 Principle of CDMA:

CDMA consists of using a code spreading technique (DS-SS), using a family of orthogonal or pseudo-orthogonal codes. It allows the simultaneous transmission of several channels each being established in time and frequency (good resistance to flat fading to fast fading).

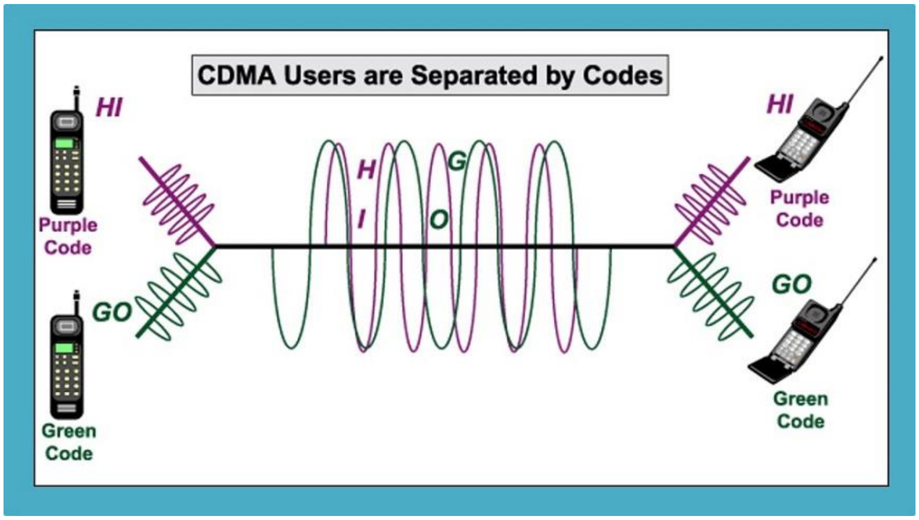


Figure II.16: CDMA example between two users.

II.4.3.2 The different standards:

II.4.3.2.1 IS-95:

Standard 95 (IS-95) ai, is the first CDMA-digital cellular standard created and deployed by Qualcomm. The brand name for IS-95 is CDMAOne. IS-95 is also known as TIA-EIA-95. It is the second generation of mobile telecommunications.

CDMA, created for digital radio, to send voice, and signaling data (such as a dialed phone number) between the mobile phone and base stations.

CDMA allows multiple MSs (Mobile Stations) to share the same frequencies while being active all the time, because network capacity does not directly limit the number of active MSs.

II.4.3.2.2 CDMA 2000:

The CDMA2000 standard, also known as IS-2000, is an evolution from CDMAOne (IS-95) to third generation services. CDMA 2000 divides the spectrum in multi-carrier lines (TDD mode). It is suitable for micro and Pico cells as well as asymmetric high-speed and asymmetric packet data traffic. Its parent wears this standard: the Qualcomm Company based in California, United States.

The main advantage of CDMA2000 over W-CDMA is its compatibility with 2G networks using the same Qualcomm technology (CDMAOne), which greatly facilitated the conversion of 2G subscribers into 3G users in certain markets (Korea, Japan and in a lesser extent in the United States

The CDMA2000 standard has already undergone several developments:

- CDMA2000 1X with an average rate of 144 Kbps in a mobile environment.
- CDMA2000 1X EV-DO: (Evolution Data Only) with an average throughput of 600 Kbps and peak speeds of up to two Mbps).
- CDMA2000 1X EV-DV: (Evolution Data and Voice) with data rate and data rates of peak of up to two to five Mbps.

II.4.3.2.3 W-CDMA:

The WCDMA standard is developed by 3GPP (3GPartnershipProject). In order to meet the requirements requested by the ITU, the 3GPP introduced its standard in several phases with annual revisions. In WCDMA mode, 3G is not compatible with 2G (GSM). Its commercial deployment

therefore presupposes the construction of new networks and obtaining new operating licenses. For the 3GPP standard.

II.4.3.3 Advantages of CDMA :

- Resistance to Interference :

Since CDMA is a spread spectrum multiplexing method, the effective jamming must be done over the entire frequency band used. Interference linked to reflection phenomena and the presence of additive noise. The first type of interference is well tolerated by CDMA, by construction, since the codes used are weakly correlated. In view of the publications to which we have had access, resistance to the second type of interference is also assured, even if we were unable to highlight it ourselves. All these considerations mean that CDMA makes it possible to guarantee high-fidelity telephony.

- Confidentiality (low probability of interception):

For both military and civilian applications, confidentiality is an important asset for a communication system. In the case of CDMA, the transmitted signal looks a lot like noise because long pseudo-random codes are used. The signal is spread uniformly over a wide spectrum: no amplitude peak is detected for a given frequency. This makes it possible to mask the presence or not of a communication. Even if we detect the existence of a communication, it is very difficult to intercept it if you do not have access to the codes used. This is one of the reasons why the army, as well as telephone operator, uses this method.

- A multiplexing adapted to the cellular system:

Current mobile phone networks are all based on the concept of cells. A cell corresponds to a geographical area in which the users all pass through the same relay. There are two problems: that of the reuse of frequencies and that of the passage of a user from one cell to another.

From the point of view of frequency reuse, CDMA shifts the problem since it is about codes and no longer frequencies.

CDMA transmission quality is only slightly affected by differences in signal amplitude from different users. This allows in practice to increase the size of the cells. The frequency of switching

from one cell to another is then reduced (for users in motion) and the risk of stalling is reduced accordingly.

- Löw consumption :

CDMA requires less power than competing technologies. This gain is present in conversation or not. This allows the increase in the autonomy of mobile phones or the reduction in the size of the batteries and therefore of the handsets. [11]

II.5 Conclusion:

Wireless networking offers many opportunities to increase productivity and reduce costs. It also changes the overall IT security risk profile of an organization. Although it is impossible to completely eliminate all risks associated with wireless networks, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to risk assessment and management. This chapter has discussed the threats and vulnerabilities associated with each of the three core technology components of wireless networks (clients, access points, and transmission medium) and described various commonly available countermeasures that could be used to mitigate these risks.

Chapter III

Wireless Network Attack Predictive System

Introduction:

With the development of artificial intelligence technology, deep learning has applied to modulation classification and achieved very good results. We introduced an improved deep neural architecture for implementing radio signal Identification tasks, which is an important facet of constructing the spectrum-sensing capability required by software-defined radio. We are currently looking via this chapter to develop our predictive system within a software environment used to build our model for that and in order to validate our results; we used one database of scientific order, code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes used to distinguish among the different users. [1]

A comparative study will presented in order to validate our results.

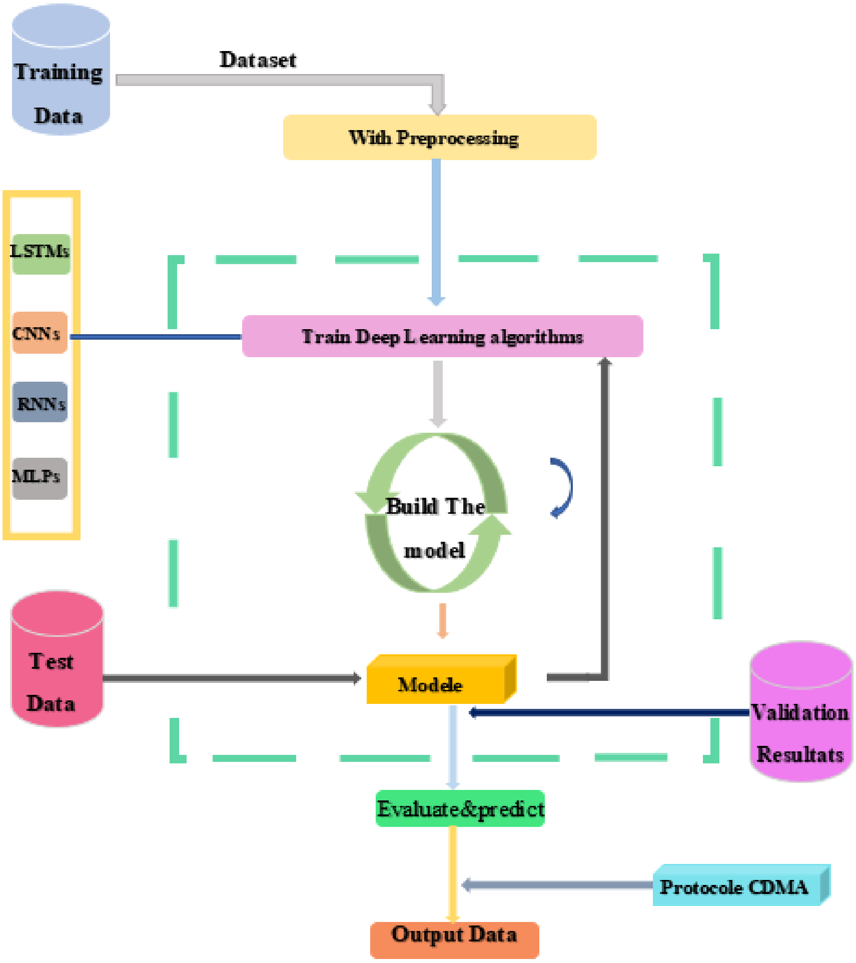


Figure III.1: Architecture of our study.

III.2 Tools and Libraries used:

III.2.1 Anaconda:

Anaconda is an open-source distribution of the Python and R programming languages for data science that aims to simplify package management and deployment. Package versions in Anaconda are managed by the package management system, anaconda, which analyzes the current environment before executing an installation to avoid disrupting other frameworks and packages.[2]

Anaconda helps in simplifying package management and deployment; it comes with a wide variety of tools easily collect data from various sources using various machine learning and AI algorithms. It helps in getting an easily manageable environment setup that can deploy any project with a single click. [3]

III.2.2 Jupyter notebook:

Jupyter is an acronym that stands for Julia, Python and R. These programming languages were the first target languages of the Jupyter application, but today, notebook technology supports many other languages as well.

As a server-client application, the Jupyter Notebook application allows us to edit and run our notebooks via a web browser.

The application can be run on a PC without Internet access, or it can be installed on a remote server, where we can access it via the Internet.

A kernel is a program that runs the user's code. The Jupyter Notebook application has a kernel for the Python code. The application dashboard not only shows you the notebook documents we have created and can reopen, but can also be used to manage the kernels: we can know which ones are running and stop them if necessary.[4]

III.2.3 Python:

Python is a versatile high-level programming language widely used in many areas such as web application development, in programs using graphical interfaces and in distributions of some operating systems.

In general, Python is a programming language that can used in many contexts and adapted to any type of use thanks to specialized libraries. It is free and open source [5]. Among the Python libraries, we have used [6] [7].

III.2.3.1 NumPy:

Is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays. It is the fundamental package for scientific computing with Python.

Besides its obvious scientific uses, Numpy can also be used as an efficient multi-dimensional container of generic data.

- To use NumPy just import it

```
# importNumpy
```

III.2.3.2 Matplotlib:

Is an amazing visualization library in Python for 2D plots of arrays Matplotlib is a multi-platform data visualization library built on NumPy arrays and designed to work with the broader SciPy stack. it was introduced by John Hunter in the year 2002.

One of the greatest benefits of visualization is that it allows us visual access to huge amounts of data in easily digestible visuals. Matplotlib consists of several plots like line, bar, scatter, histogram etc.

III.2.3.3 Keras:

Is a python based open-source library used in deep learning (for neural networks).It can run on top of TensorFlow, Microsoft CNTK or Theano. It is very simple to understand and use, and suitable for fast experimentation. Keras models can run on both CPU as well as GPU.

III.2.3.4 Pickle and cPickle:

Is a powerful library that can serialize many complex and custom objects that other library fails to do. Just like pickle, there a cPickle module that shares the same methods as pickle, but it written in C. The cPickle module written as a C function instead of a class format.

Difference between Pickle and cPickle:

- Pickle uses python class-based implementation while cPickleis written as C functions. As a result, cPickle is many times faster than pickle.
- Pickle is available in both python 2.x and python 3.x while cPickle is available in python 2.x by default. To use cPickle in python 3.x, we can import _pickle.
- cPickle does not support subclass from pickle. cPickle is better if subclassing is not important otherwise Pickle is the best option.etc. [8]

III.2.3.5 Tensorflow:

Is an open-source library that is developed by Google for running machine learning models as well as deep learning neural networks in the browser or node environment.

The if Model () function is used to create a model which contains layers and layers that are provided in form of input and output parameters.

III.2.3.6 scikit-learn:

Is an open-source Python library that implements a range of machine learning, pre-processing, cross-validation, and visualization algorithms using a unified interface?

Important features of scikit-learn:

- Simple and efficient tools for data mining and data analysis. It features various classification, regression and clustering algorithms including support vector machines, random forests, gradient boosting, k-means, etc.
- Accessible to everybody and reusable in various contexts.
- Built on the top of NumPy, SciPy, and matplotlib.
- Open source, commercially usable – BSD license.

II.2.4 Classification of Modulation Techniques:

Modulation is the process of varying some parameter of a periodic waveform in order to use that signal to convey a message. Normally a high-frequency sinusoidal waveform is used as carrier signal. For this purpose ,if the variation in the parameter of the carrier is continuous in accordance to the input analog signal the modulation technique is termed as analog modulation scheme if the variation is discrete then it is termed as Digital Modulation Technique.

III.2.4.1 Analog Modulation Techniques:

There are basically three type of analog modulation schemes the amplitude modulation the Frequency modulation and the phase modulation.

III.2.4.1.1 Modulation AM-DSB:

It is a double sideband with carrier AM and his bandwidth = 2fm, be can less number of channels in a given frequency range and moderate power consumption and moderately difficult reconstruction, be moderately redundant data, and be tracking might be required. [9]

III.2.4.1.2 Modulation AM-SSB:

It is only one side band AM, without carrier ,and his bandwidth = fm, be can more number of channels in a given frequency range ,and least power consumption and difficult reconstruction ,be least redundant data ,and be synchronization or tracking is essential.[9]

III.2.4.1.3 Modulation WB-FM:

Wideband FM defined as the situation where the modulation index is above 0.5. Under these circumstances, the sidebands beyond the first two terms are not insignificant. Broadcast FM stations use wideband FM, and using this mode they are able to take advantage of the wide bandwidth available to transmit high quality audio as well as other services like a stereo channel, and possibly other services as well on a single carrier.[10]

III.2.4.2 Digital Modulation Techniques:

After the conversion of an Analog signal to digital by sampling different type of digital modulation, schemes can achieved by the variation of different parameter.

III.2.3.2.1 Modulation 8PSK:

It uses 8PSK modulation in order to achieve a higher data transmission rate. The modulation format changed to 8PSK from GMSK. This provides an advantage as it is able to convey 3 bits per symbol, and increases the maximum data rate. However, this upgrade required a change in the base station [8].

III.2.4.2.2 Modulation BPSK:

BPSK also known as phase reversal keying or 2PSK is the simplest form of phase shift keying. The Phase of the carrier wave changed according to the two binary inputs. In Binary Phase shift keying, difference of 180-phase shift is used between binary 1 and binary0.

This regarded as the most robust digital modulation technique and is used for long distance wireless communication [8].

III.2.4.2.3 Modulation CPFSK:

Continuous-phase frequency-shift keying (CP-FSK) is binary FSK except the mark and space frequencies synchronized with the input binary bit rate. With CP-FSK, the mark and space frequencies are selected such that they are separated from the center frequency by an exact multiple of one-half the bit rate (fm and fs = n[fb / 2]), where n = any integer).[11]

III.2.4.2.4 Modulation GFSK:

GFSK encoded in the form of variations of frequency in a carrier in a similar manner to FSK. Therefore, the modulator used can be the same that used for FSK modulation. However, the impulses pass through a Gaussian filter before entering the pulse modulator to decrease the spectral width of the same. The Gaussian filter is a kind of pulse formatter used to smooth the transition between the values of the impulses. [12]

III.2.4.2.5 Modulation PAM4:

PAM4 is a branch of the pulse amplitude modulation (PAM) technology, which is a mainstream signal transmission technology following non-return-to-zero (NRZ). Playing a key role in multi-order modulation, PAM is widely used in high-speed signalinter connection.[13]

III.2.4.2.6 Modulation QAM16:

16-QAM is an M-ary system where M = 16, the input data are acted on in groups of four (2^4=16). As with 8-QAM, both the phase and the amplitude of the transmit carrier are varied.[11]

III.2.4.2.7 Modulation QAM64:

64-QAM is an M-ary system where M = 64, the input data are acted on in groups of four (2^6=64). As with 8-QAM, both the phase and the amplitude of the transmit carrier are varied.[11]

III.2.4.2.8 Modulation QPSK:

QPSK is an M-ary encoding scheme where N = 2 and M= 4 (hence, the name "quaternary" meaning "4"). A QPSK modulator is a binary (base 2) signal, to produce four different input combinations: 00, 01, 10, and 11.

Therefore, with QPSK, the binary input data combined into groups of two bits, called debits. In the modulator, each debit code generates one of the four possible output phases (+45°, +135°, -45°, and -135°).[11]

III.3 Evaluation Dataset:

III.3.1 Dataset Parameters:

We use the dataset in each sample and the dataset consists of 128 complex valued data points, each data point has the dimensions of (128, 2, 1) to represent the real and imaginary components. We use 11 modulations: 8 digital and 3 analog modulation, (BPSK, QPSK, 8PSK, QAM16, QAM64, CPFSK, GFSK, PAM4, WBFM, AM-SSB, and AM-DSB) collected over a wide range of SNRs from -20 dB to 18 dB in 2 dB increments. These modulations categorized into signal types.We consider different modulation schemes used by different types of users transmitting on a single channel. We start with the baseline case where modulations used by different user types known and there is no signal superposition we categorize modulations into four signal types:

1) Idle: no signal.
2) In-network user signals: QPSK, 8PSK, CPFSK, BPSK.
3) Jamming signals: QAM16, QAM64, PAM4, and WB-FM.
4) Out-network user signals: AM-SSB, AM-DSB, and GFSK.

There are in-network users (trying to access the channel opportunistically), out-network users (with priority in channel access) and jammers that all coexist. Out-network users are treated as primary users and their communications should be protected. Without prior domain knowledge other than training data, an in-network user classifies received signals to idle, in-network, jammer, or out-network. At each SNR, there are 1000 samples from each modulation type, Instead of using a conventional feature extraction or off-the-shelf deep neural network architectures such as ReseNt, we build a custom deep neural network that takes I/Q data as input.[14]

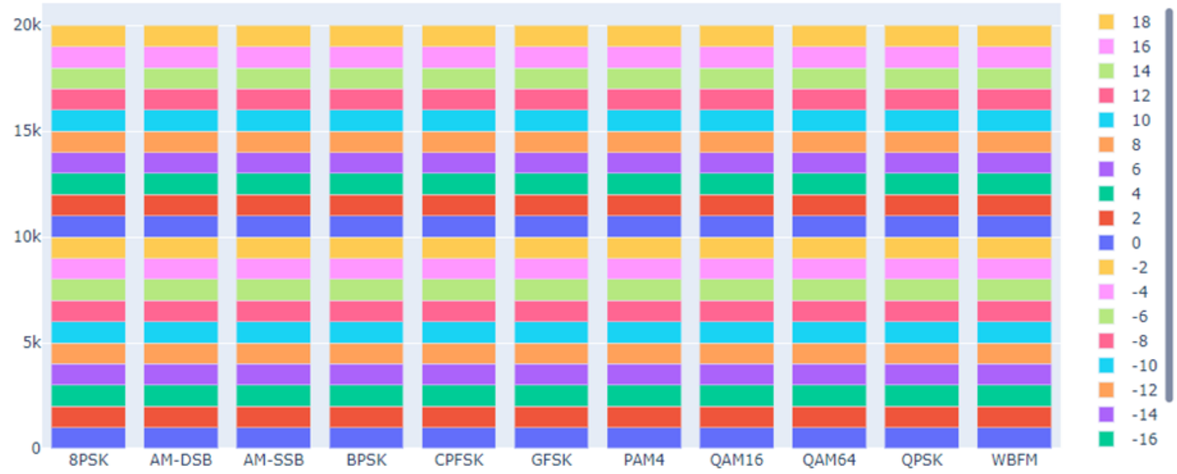


Figure III.2: SNR according to function of modulation classification

TableIII.1: Dataset Parameters.

Dataset	**RadioML2016.10.a**
Modulations	8 Digital Modulations: BPSK, QPSK, 8PSK, 16QAM, 64QAM, BFSK, CPFSK, and PAM4 3 Analog Modulations: WBFM, AM-SSB, and AM-DSB
Length per sample	128
Signal format	In-phase and quadrature (IQ)
Signal dimension	2×128 per Sample
Duration per sample	128 µs
Sampling frequency	1 MHz
Samples per symbol	8
SNR Range	[-20 dB, -18 dB, -16 dB, . . ., 18 dB]
Total number of samples	220000 vectors
Number of training samples	198000 vectors
Number of test samples	22000 vectors

III.3.2 Data visualization:

Data visualization is an imperative aspect of data science. It helps to understand the data and to explain it. When we encounter a dataset, we must first analyze and “get to know” the dataset. Inspecting a single example from each class of modulation in the time, we see a number of similarities and differences between modulations visually, but due to pulse shaping, distortion and other channel effects they are not all readily discernible.

Signal Module: In digital and analog communications, modulation often expressed in terms of Q, the I and I axis lies on the zero degree phase reference, and the Q axis is rotated by 90 degrees. The signal vector’s projection onto the I axis is its “I” component and the projection onto the Q axis is its “Q” component. [15]

Instead of using a conventional feature extraction or off-the-shelf deep neural network architectures such as ResNet, we build a custom deep neural network that takes I/Q data as input.

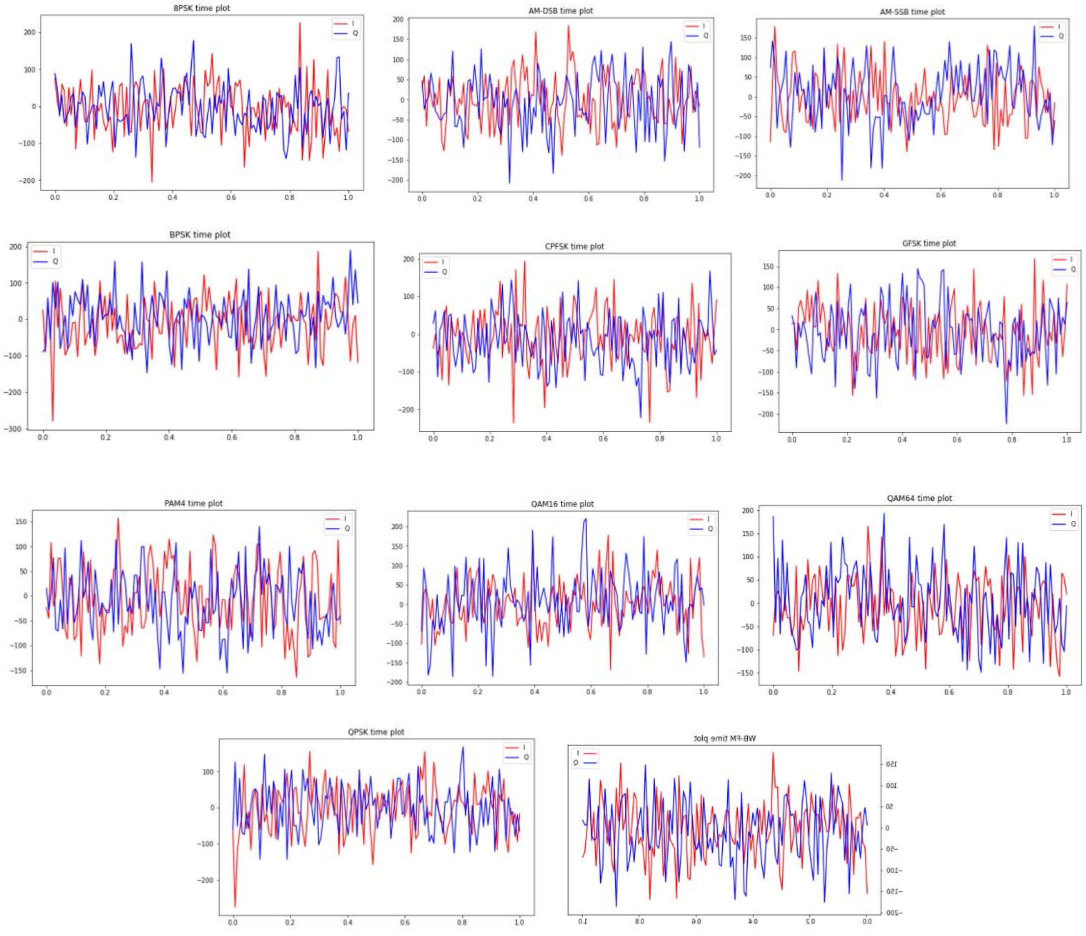


Figure III.3: Time Domain of High-SNR.

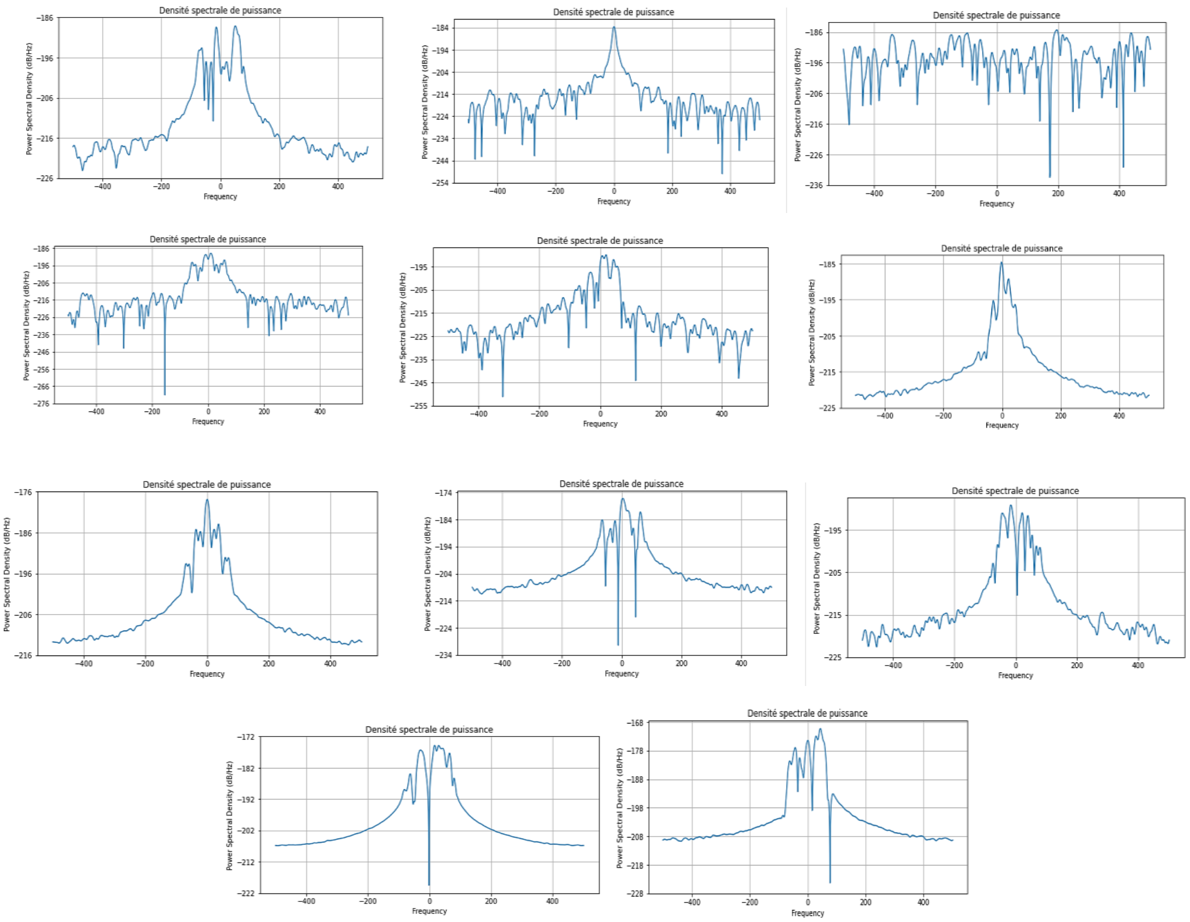
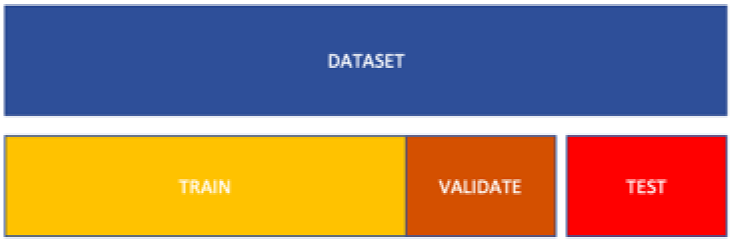


Figure III.4: Power Spectrum of High-SNR.

III.4 Evaluation methods:

III.4.1 Training Parameters:

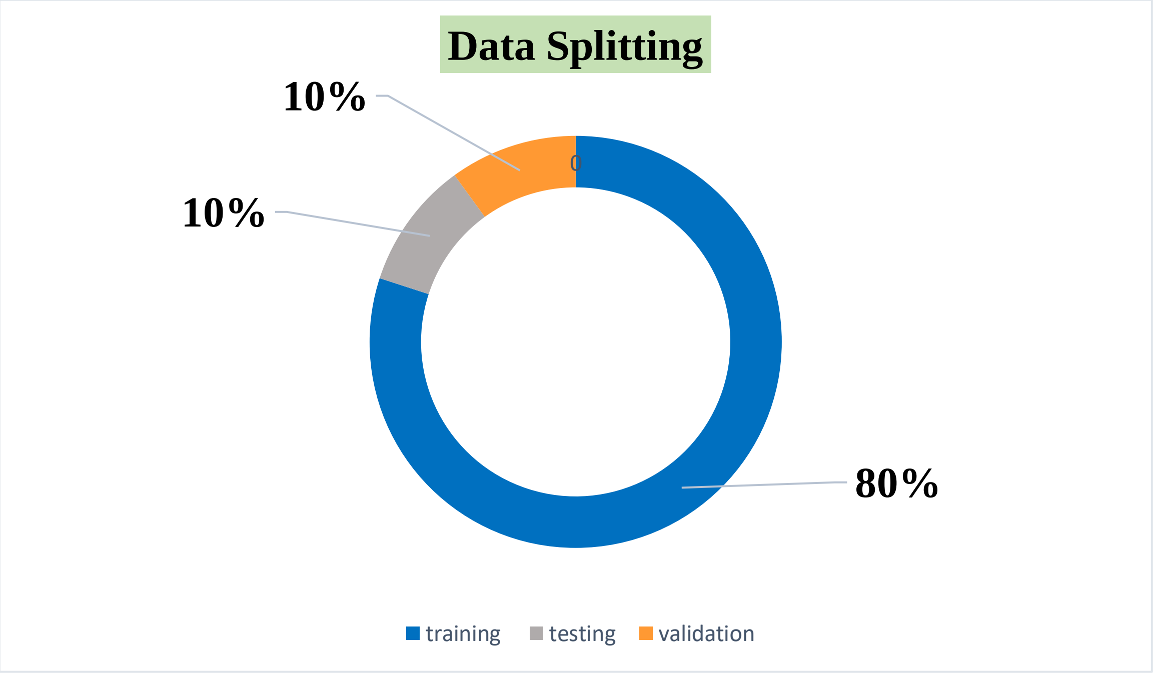
- Number of Epochs: 50
- Adam Optimizer utilizing a learning Rate of choice: 0.005 (Also tried 0.03, 0.01 and 0.0001).
- Dropout of choice 0.5 (Also tried 0.4 and 0.6).
- Training Batch Size: 10.
- 80% of data set is used of training.
- 10% of data set is used of validation.
- 10% of data set is used of testing.



FigureIII.5: Principle of the Train/Test Split method.

III.4.2 Train/Test Split:

This method the classifier is trained in Tensor Flow the ADAM optimizer is used with a step size of$\mathbf{5\times10^{-5}}$and the categorical cross-entropy loss function is used for training we split the data into 80% for training and 10% for testing and 10% foe validation.



FigureIII.6: Data Splitting.

III.4.3 Measures of Precision:

A confusion matrix is an extremely useful tool to observe in which way the model is wrong (or right!), it is a matrix that compares the number of predictions for each class that are correct and those that are incorrect.

In a confusion matrix, there are four numbers to pay attention to.

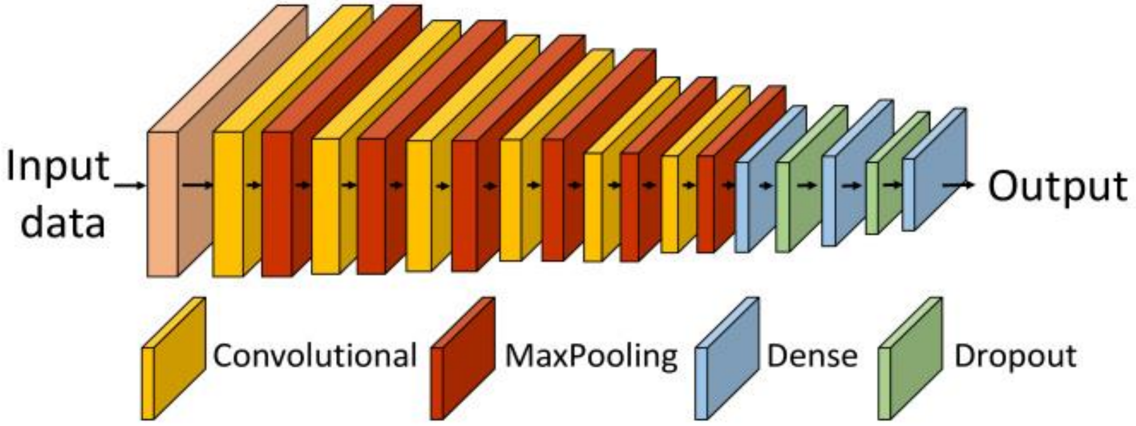
- True Positives: The number of positive observations the model correctly predicted as positive.(TP)
- False Positive: The number of negative observations the model incorrectly predicted as positive.(FP)
- True Negative: The number of negative observations the model correctly predicted as negative.(TN)
- False Negative: The number of positive observations the model incorrectly predicted as negative.(FN)
- Precision (P), Recall (R).

Table III.2: Precision measurements

performance metrics	Definition	Formula
Accuracy	accuracy of a model is simply the number of correct predictions divided by the total number of predictions	A= (TP+TN) / (Total number of samples)
Recall	Recall tell us how good the model is at correctly predicting all the positive observations in the dataset.	R =TP / (TP+FN)
F1 score	The F1 score is the harmonic mean of precision and recall	F=2*[(P*R) / (P+R)]
Precision	Precision measures how good the model is in correctly identifying the positive class.	P = TP / (TP+ FP)

III.4.4 Method Evaluation Model:

We train a CNN classifier that consists of several convolutional layers and fully connected layers in the last three stages. However, when the filter size in the convolutional layers is not divisible by the strides, it can create checkerboard effects In the CNN classifier structure; we paid attention to avoid the checkerboard effects and used the following layers. [14]



FigureIII.7: CNN classifier structure for RF signal classification**.**

- Input shape: (128, 2).
- 2D ZeroPadding with size (1, 1).
- Convolutional layer with 128 filters with size of (3, 3).
- 2D MaxPolling layer with size (2, 1) and stride (2, 1).
- Five cascades of the following:
  - ✓ 2D Zero padding with size (1, 1)
  - ✓ Convolutional layer with 256 filters with size of (3, 3).
  - ✓ 2D Max Polling layer with pool size (2, 2) and stride (2, 1).
- Fully connected layer with 256 neurons and Scaled Exponential Linear Unit (Relu) activation function, which is $\mathbf{x}$ if $\mathbf{x} > \mathbf{0}$ and $\mathbf{a}\ e^{x} - \mathbf{a}$ if $\mathbf{x} \leq \mathbf{0}$ for some constant **a**.
- Dropout with probability 0.5.
- Fully connected layer with 64 neurons and Relu activation function.
- Dropout with probability 0.5.
- Fully connected layer with 4 neurons and Relu activation function

III.5 Results and Discussions:

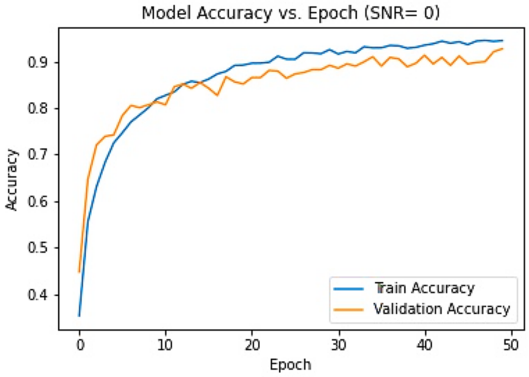
Experiments performed using Intel Core(TM) i5-8265U processor with 8 GB RAM and NVidia. The model trained via Adam optimizer with an initial learning rate of 0.001. The Sparse Categorical Cross entropy used as loss functions and it the optimization algorithm, the error for the current state of the model estimated repeatedly. This requires the choice of an error function, conventionally called a loss function that used to estimate the loss of the model so that the weights updated to reduce the loss. The number of batch size is 10. The performance of the proposed model has been evaluated using accuracy; the accuracy defined as, on average, how far your measurements or results are from your target. In other words, accuracy is the extent to which the average of the measurements deviate from the true value.

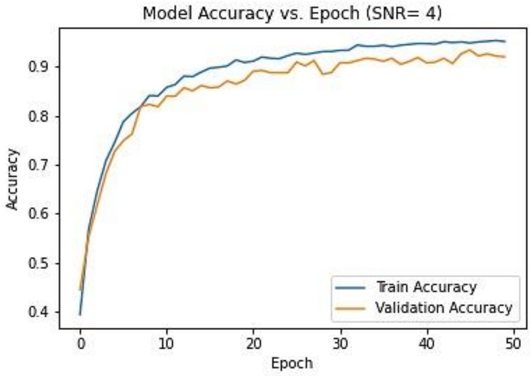
In order to evaluate the performance of the proposed model, comparison conducted against state-of-the-art [14]

III.5.1 Model Accuracy and Loss vs. Epoch (SNR):

We have plotted the accuracy and loss curves of the CNN model used for each SNR values for both training and validation sets, shown by (Figure III.8, Figure III.9) and (Figure III.10, Figure III.11) respectively. (See all the curves in **Annex 1**).

- ✓ **Model Accuracy vs. Epoch:**
  - **SNR (positive):**





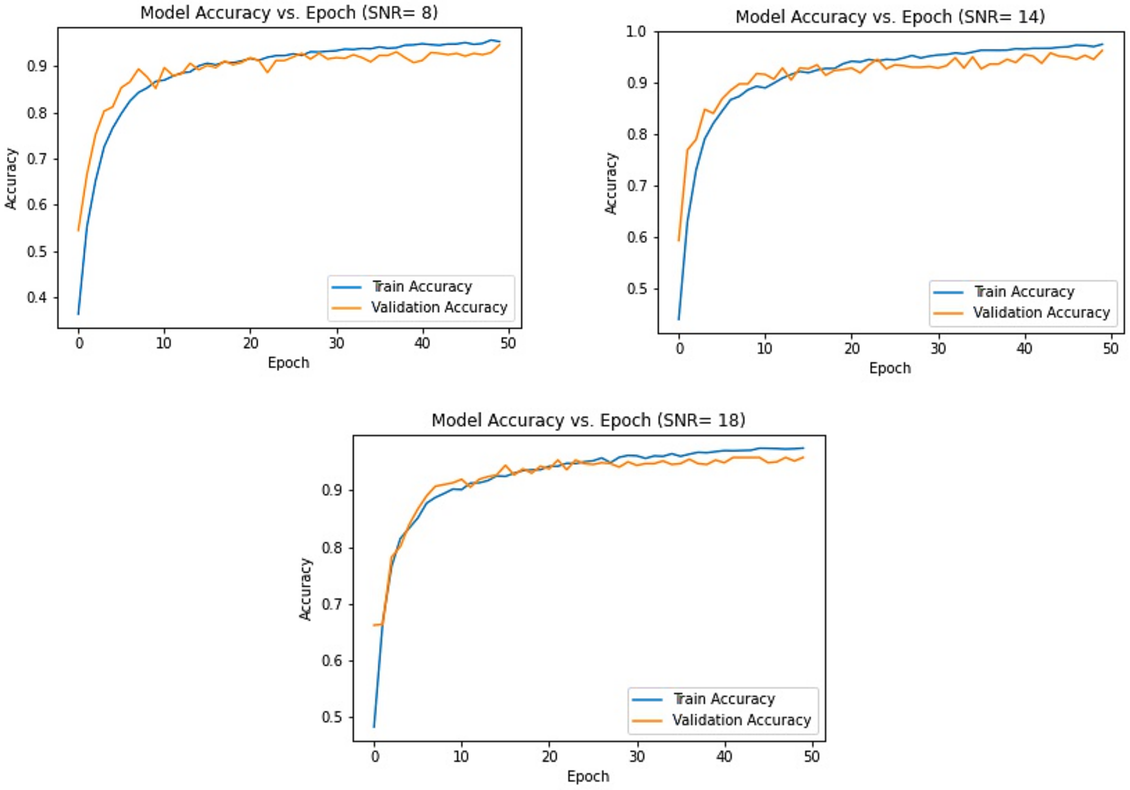


Figure III.8: Model Accuracy vs. Epoch in SNR (positive).

Table III.3: Accuracy with change in SNR values (positive)

SNR	Accuracy	SNR	Accuracy
0	0.9185	10	0.9740
2	0.8889	12	0.9691
4	0.9395	14	0.9518
6	0.9518	16	0.9660
8	0.9383	18	0.9606

- **SNR (negative):**

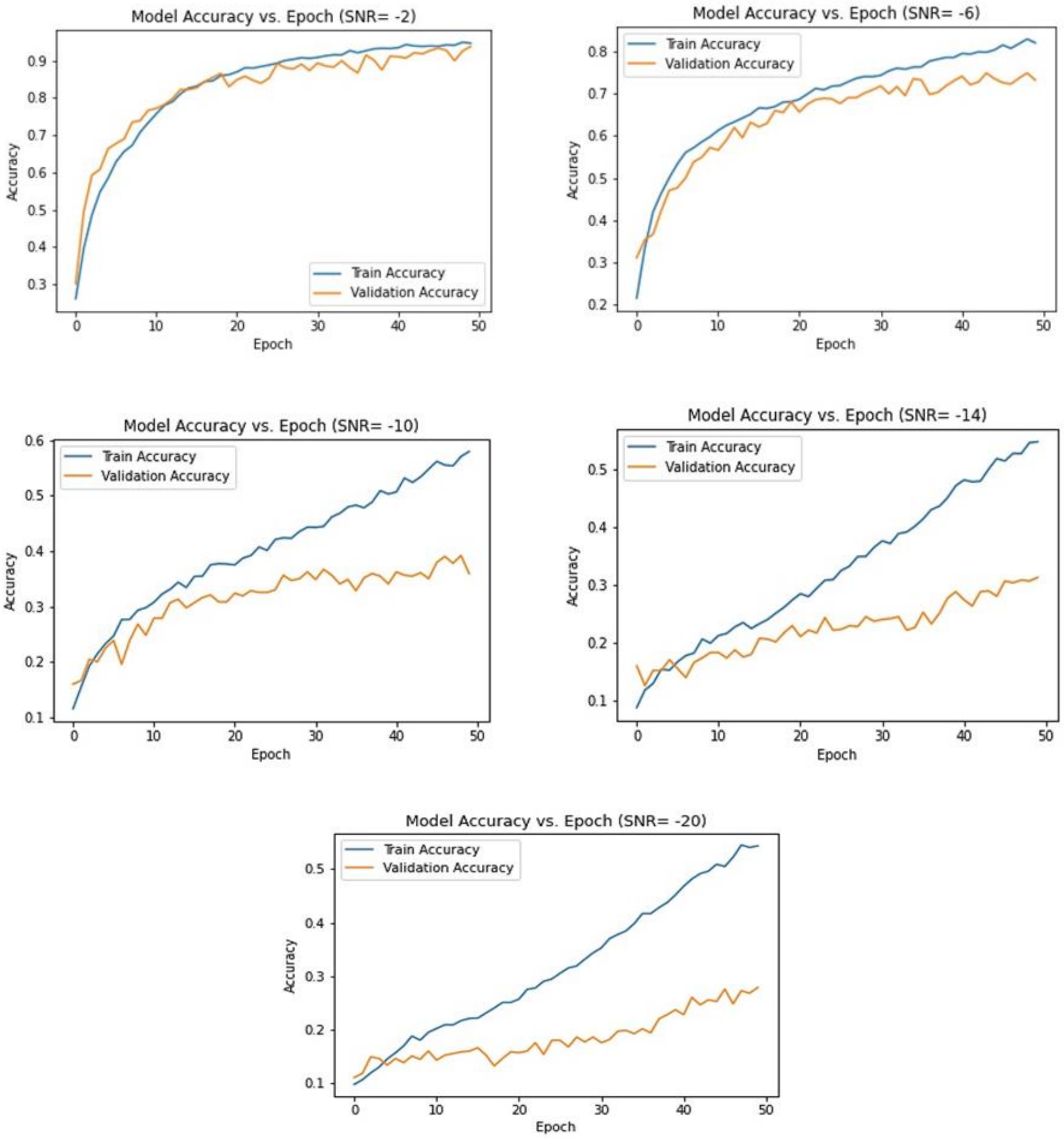


Figure III.9: Model Accuracy vs. Epoch in SNR (negative).

Table III.4: Accuracy with change in SNR values (negative).

SNR	Accuracy	SNR	Accuracy
-2	0.9358	-12	0.3615
-4	0.8624	-14	0.2973
-6	0.7495	-16	0.2924
-8	0.6372	-18	0.2720
-10	0.4324	-20	0.3096

- ✓ **Model Loos vs Epoch:**

- **SNR (positive):**

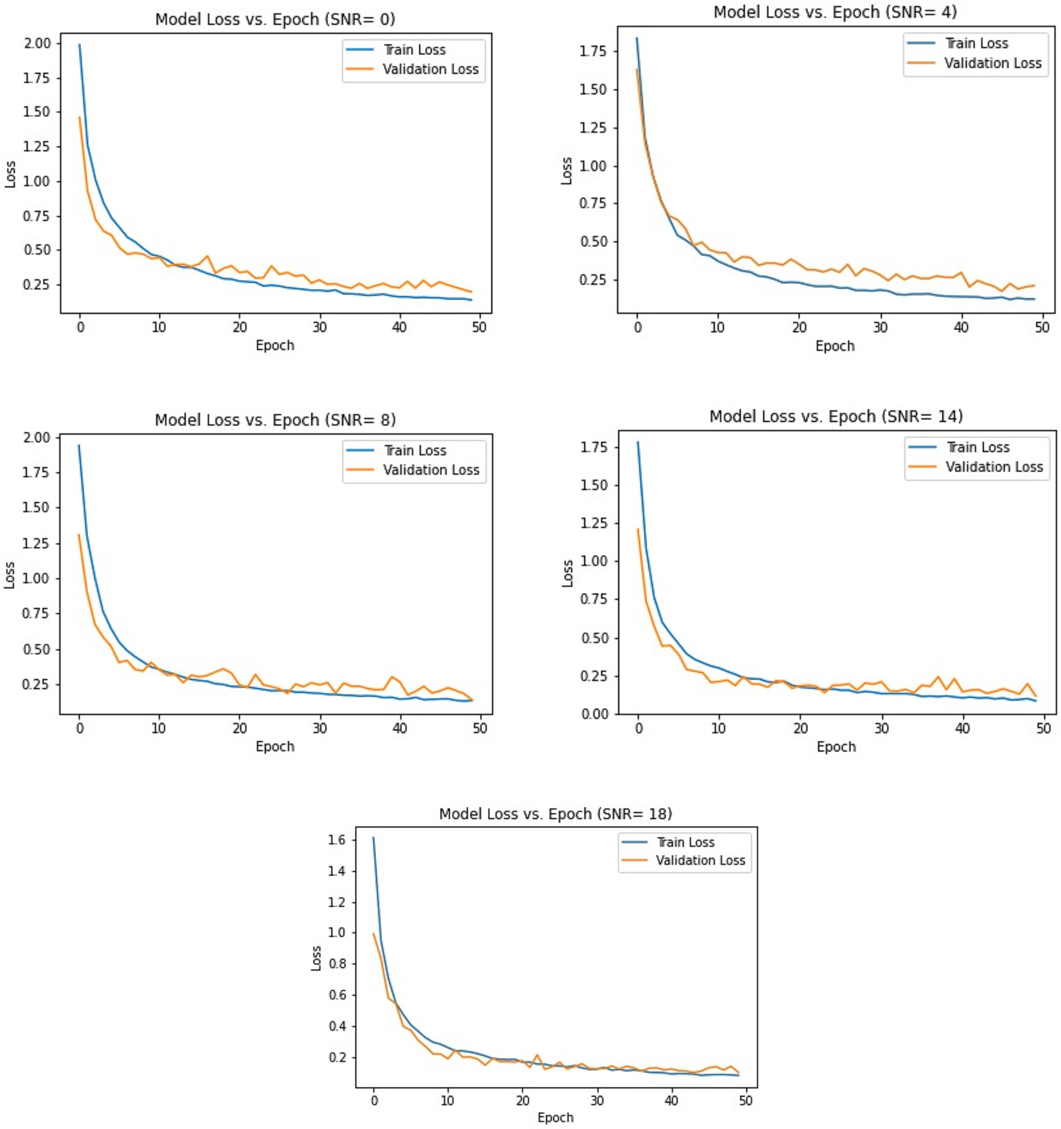


Figure III.10: Model Loss vs. Epoch in SNR (positive).

- **SNR (negative) :**

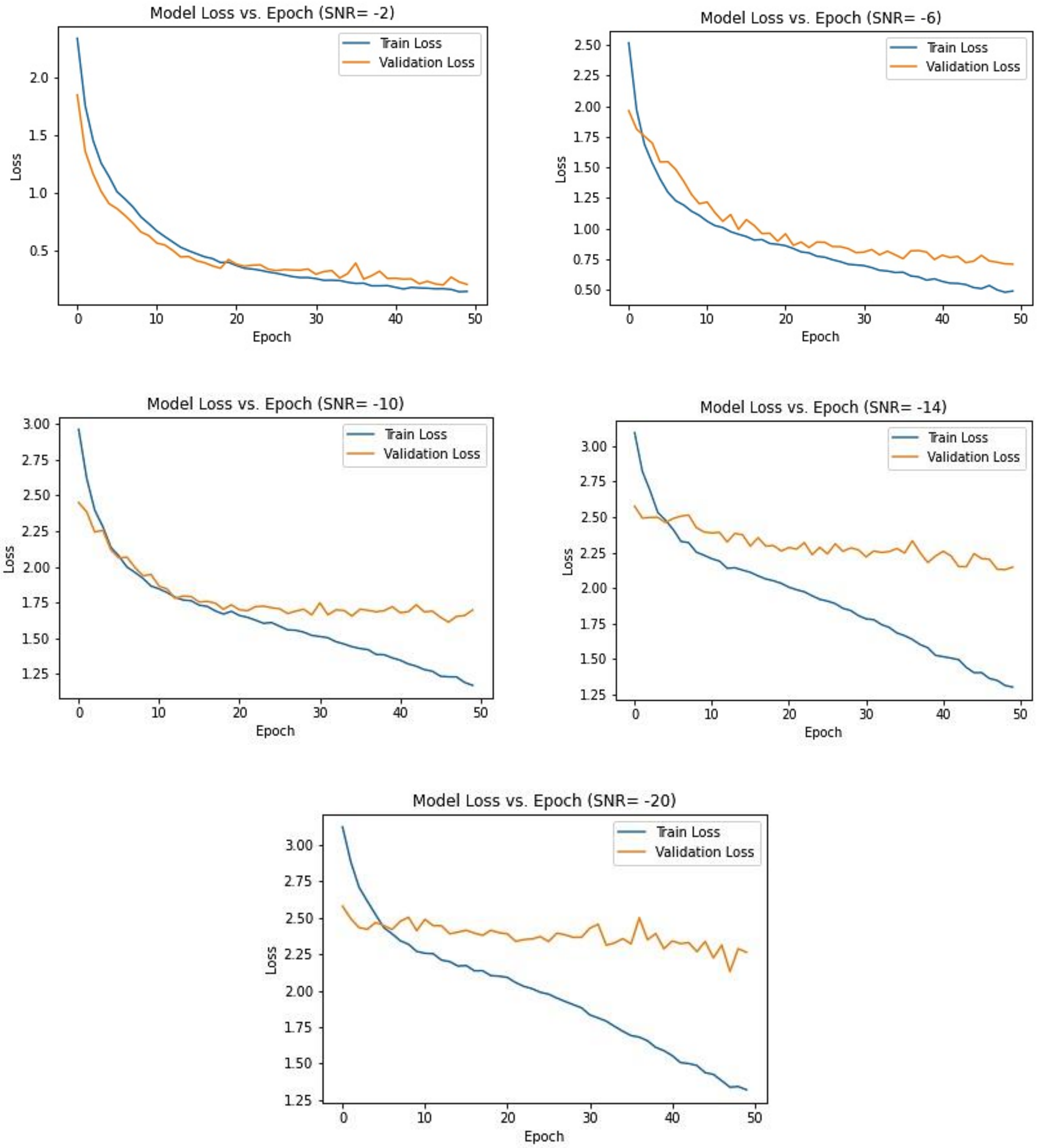


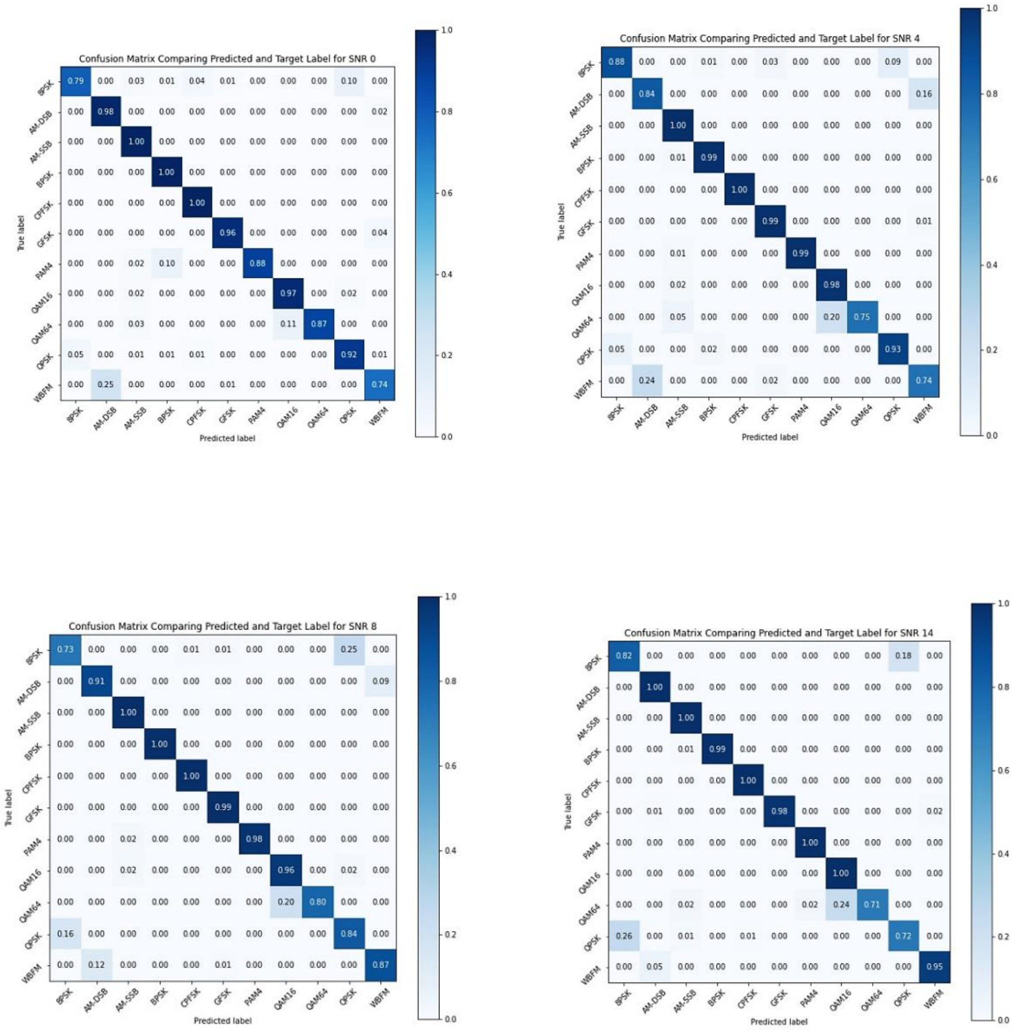
Figure III.11: Model Loss vs. Epoch in SNR (negative).

- **Comment (Accuracy and Loss):**

We have rehearsed 80% of the data on 50epochs, where we note that high or positive SNR values give us very good results (accuracy and loss) compared to the results of negative SNR values, which gave us results less than positive SNR values in terms of (accuracy and loss) and are not appropriate.

III.5.2 the Results of Confusion Matrix:

A confusion matrix is a technique for summarizing the performance of a classification algorithm. Classification accuracy alone can be misleading if we have an unequal number of observations in each class. Calculating a confusion matrix can give we a better idea of what classification model is getting right and what types of errors it is making. We have the results of the noise matrix for all positive and negative SNR values as shown in FigureIII.12 and FigureIII.13.



Confusion Matrix Comparing Predicted and Target Label for SNR 0

True label \ Predicted label	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.79	0.00	0.03	0.01	0.04	0.01	0.00	0.00	0.00	0.10	0.00
AM-DSB	0.00	0.98	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.96	0.00	0.00	0.00	0.00	0.04
PAM4	0.00	0.00	0.02	0.10	0.00	0.00	0.88	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.97	0.00	0.02	0.00
QAM64	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.11	0.87	0.00	0.00
QPSK	0.05	0.00	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.92	0.01
WBFM	0.00	0.25	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.74

Confusion Matrix Comparing Predicted and Target Label for SNR 4

True label \ Predicted label	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.88	0.00	0.00	0.01	0.00	0.03	0.00	0.00	0.00	0.09	0.00
AM-DSB	0.00	0.84	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.16
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.01	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.99	0.00	0.00	0.00	0.00	0.01
PAM4	0.00	0.00	0.01	0.00	0.00	0.00	0.99	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.98	0.00	0.00	0.00
QAM64	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.20	0.75	0.00	0.00
QPSK	0.05	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.93	0.00
WBFM	0.00	0.24	0.00	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.74

Confusion Matrix Comparing Predicted and Target Label for SNR 8

True label \ Predicted label	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.73	0.00	0.00	0.00	0.01	0.01	0.00	0.00	0.00	0.25	0.00
AM-DSB	0.00	0.91	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.09
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.99	0.00	0.00	0.00	0.00	0.00
PAM4	0.00	0.00	0.02	0.00	0.00	0.00	0.98	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.96	0.00	0.02	0.00
QAM64	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.20	0.80	0.00	0.00
QPSK	0.16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.84	0.00
WBFM	0.00	0.12	0.00	0.00	0.00	0.01	0.00	0.00	0.00	0.00	0.87

Confusion Matrix Comparing Predicted and Target Label for SNR 14

True label \ Predicted label	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.82	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.18	0.00
AM-DSB	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.01	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.01	0.00	0.00	0.00	0.98	0.00	0.00	0.00	0.00	0.02
PAM4	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
QAM64	0.00	0.00	0.02	0.00	0.00	0.00	0.02	0.24	0.71	0.00	0.00
QPSK	0.26	0.00	0.01	0.00	0.01	0.00	0.00	0.00	0.00	0.72	0.00
WBFM	0.00	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.95

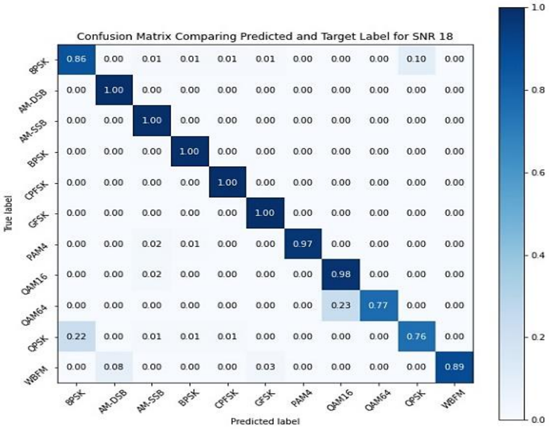
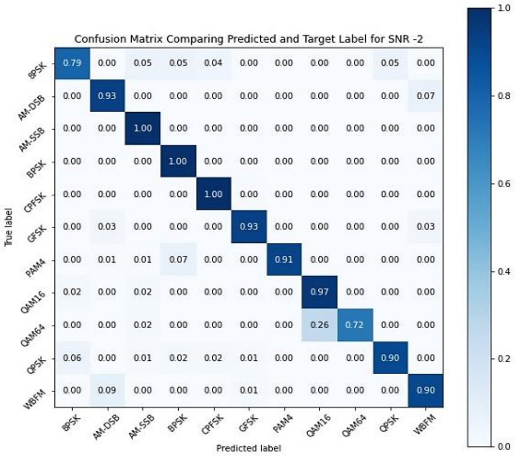
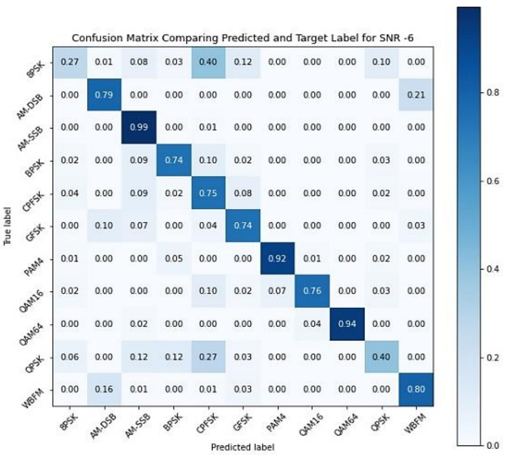
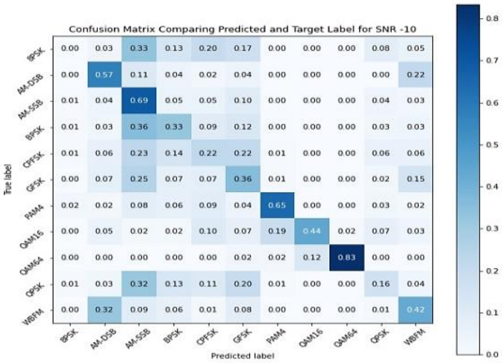
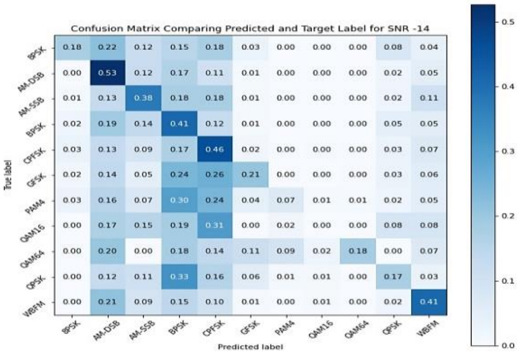


Figure III.12 : Confusion matrix in SNR (positive).









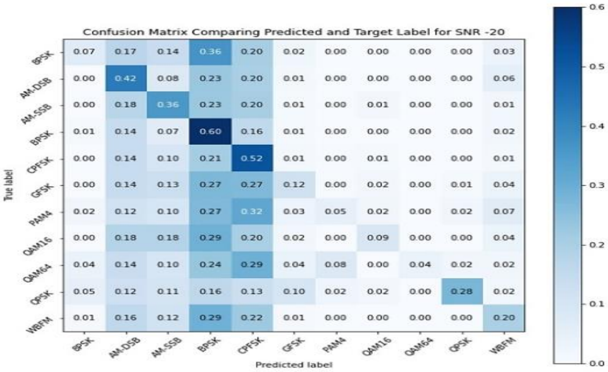


Figure III.13: Confusion matrix in SNR (negative).

- **Comment Confusion Matrix:**

Figure 11 shows the normalized classification of each kind of modulated signal including 8PSK, AM-DSB, BPSK, CPFSK, GFSK, PAM4, QAM16, QAM64, QPSK, and WBFM by the six methods when the SNR is 18 db. In Figure 11, the vertical column represents the true label of the modulated signal and the horizontal row represents the predicted label gotten from the deep neural network. All data normalized. In this connection, the data on the diagonal is the classification accuracy. For example, in Figure 11(SNR=4), there are two non-zero values in the top row, that is, 0.88 and 0.05, which indicates that the classification accuracy is 95% for 8PSK modulated signal by the proposed method and there are 5% 8PSK signals that are recognized as QPSK signals. In this connection, it found that the classification accuracy of 8PSK, BPSK, CPFSK, GFSK, PAM4, QAM16, QAM64, QPSK, and WBFM gotten from the proposed method is highest among the six methods when the SNR is 18 dB

The negative SNR values has small accuracies, 53% for SNR= -14 and 74% for SNR=0, the accuracy improves with higher SNR values, as we can see we get 83% for SNR=2 **(see all the CM results in annex 2**).

III.5.3 Performance of all Trained Models of Dataset:

It seen that the classification accuracy of each modulation type using the six methods shows a general upward trend gradually and fluctuates within a narrow range with the increase of SNR, the following curve presents the accuracy of the proposed system, which we can divide into three phases as follows:

- **The first phase** (from -20 to -10):

  We can notice in the SNR values between -20 and -10 a slow increase in the accuracy ratio from 29% to 40%.
- **The second phase**(from -10 to 0):

  At this point, we notice a very rapid increase in accuracy from 40% to 90%, which lies between the values of SNR-10 and .0
- **The third phase** (from 0 to 18):

  As for this stage, we notice stability or stability in the accuracy ratio, whose values lie between 90% and 100% in the SNR range, whose values are between 0 and 18.

We can see the difference between accuracy and change in signal-to-noise ratio (SNR) whether it is positive or negative in the following table.

Table III.5: Accuracy with change in SNR values (positive and negative).

SNR	Accuracy	SNR	Accuracy
0	0.9185	-2	0.9358
6	0.9518	-8	0.6372
12	0.9691	-12	0.3615
16	0.9660	-16	0.2924
18	0.9605	-20	0.3096

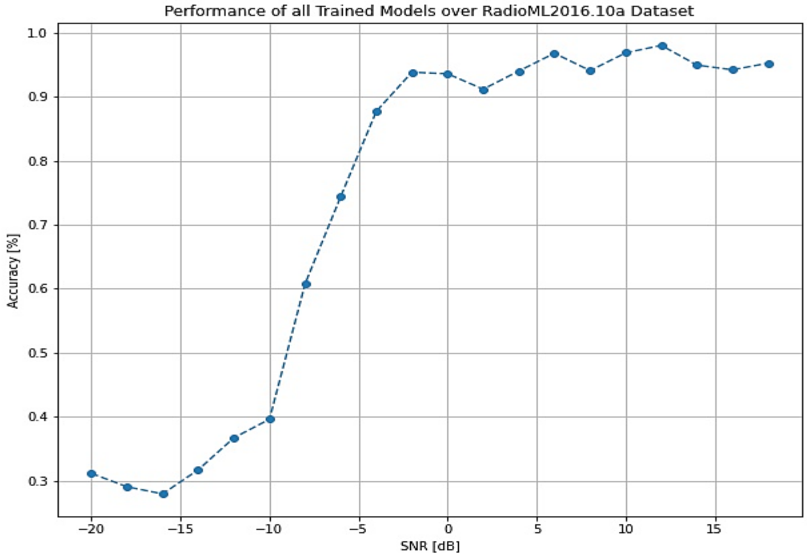


Figure III.14: Performance of all trained Models over dataset

III.5.4 Comparison of results:

In this part, we compared the results of the study with the results of another model, taking into account the use of the same data.

The following table shows us a comparison of the results:

Table III.6: Comparison of results with other models.

Reference	Type of Data	Method of algorithm	Train/test split size	Number epochs	Resultats
[21]	RadioML2016.10.a	CNN	128	100	88%
Our study	RadioML2016.10.a	CNN	10	50	99.1%

- **Observation:**

The experiment shows that the classification accuracy of the proposed method is highest with the varying SNR and it peaks at 99.1% when the SNR is 14 dB and is 11% percent higher than that of the model another .The proposed method has excellent performance for modulation classification.

IIII.5.5 Discussions:

In this study, we proposed a convolutional neural network model to identify intruder attacks for wireless networks. This model of CNN used to explore its performance in identifying these attacks. In our model, we categorize analog and digital mods as follows:

Idle: No signal. In-network user signals: QPSK, 8PSK, CPFSK, BPSK or jamming signals: QAM16, QAM64, PAM4, WB-FM or off-network user signals: AM-SSB, AM-DSB, and GFSK.

Our results show that recognition accuracy is directly related to SNR especially those with high or positive SNR will increase accuracy by a significant amount to improve model quality and reduce prediction error by using SNR.

III.6 Implementation of the contribution:

In this section, we will first define the tools used for development our application. In the second step, we will describe integrating a protocol CDMA with Deep learning.

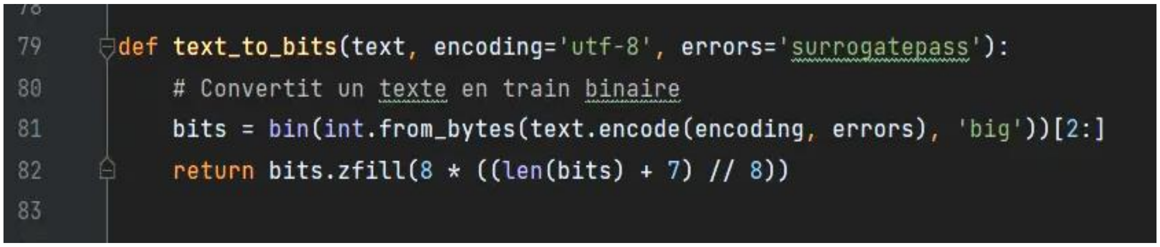
III.6.2 Description of program:

As part of the smooth running of our project and simulating the principle behind CDMA multiple access technology, we followed the following steps.

III.6.2.1 in context:

- ***Binary conversion :***

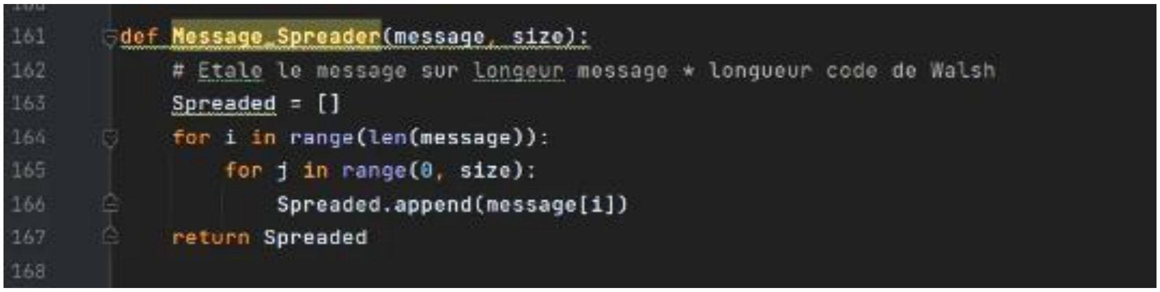
In our program, the user has the option to enter a text message directly so first we need to turn this message into a binary stream.



```
def text_to_bits(text, encoding='utf-8', errors='surrogatepass'):
    # Convertit un texte en train binaire
    bits = bin(int.from_bytes(text.encode(encoding, errors), 'big'))[2:]
    return bits.zfill(8 * ((len(bits) + 7) // 8))
```

- ***Message spreading:***

The message spread bit by bit according to the length of the Walsh code used.



```
def Message_Spreader(message, size):
    # Etale le message sur longeur message * longueur code de Walsh
    Spreaded = []
    for i in range(len(message)):
        for j in range(0, size):
            Spreaded.append(message[i])
    return Spreaded
```

The Walsh code :

The Walsh code is a linear code1, which maps binary strings of length n to binary code words of length 2 n. Further, these codes are mutually orthogonal. [16]

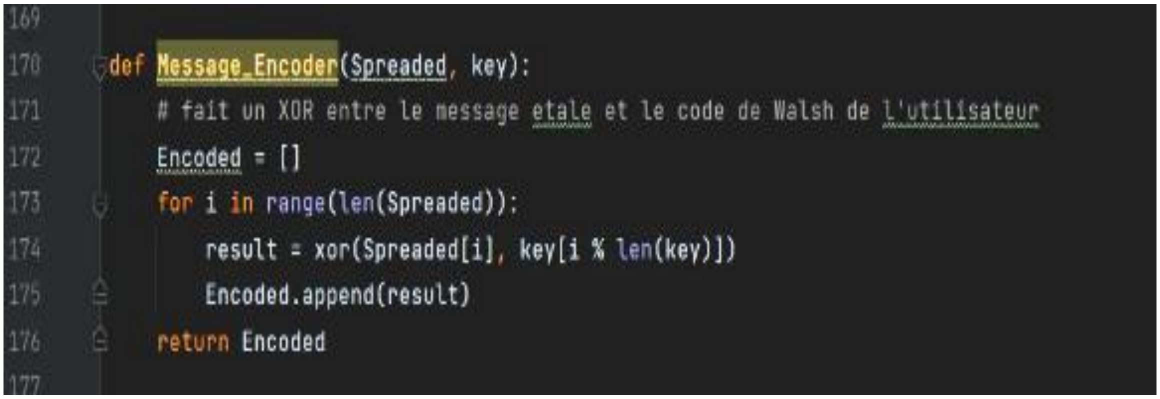
Orthogonal codes are easily generated by starting with a seed of zero, repeating the zero horizontally and vertically, and then complementing the 1 diagonally. This process continued with the newly generated block until the desired codes with the proper length generated. Sequences created in this way referred as “Walsh” code.

The Walsh code used to separate the user in the forward CDMA link. In any given sector, each forward code channel assigned a distinct Walsh code.

Message encoding:

Encoding is the process of turning thoughts into communication. The encoder uses a ‘medium’ to send the message — a phone call, email, text message, face-to-face meeting, or other communication tool. The level of conscious thought that goes into encoding messages may vary. The encoder should also take into account any ‘noise’ that might interfere with their message, such as other messages, distractions, or influences. [17]

At this level, we have defined an XOR operation to encode the message.

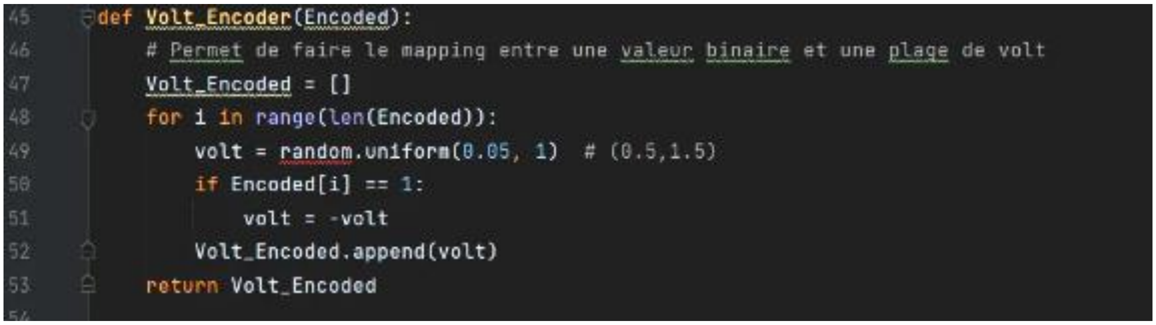


```
def Message_Encoder(Spreaded, key):
    # fait un XOR entre le message etale et le code de Walsh de l'utilisateur
    Encoded = []
    for i in range(len(Spreaded)):
        result = xor(Spreaded[i], key[i % len(key)])
        Encoded.append(result)
    return Encoded
```

- ***Convert to voltage :***

The message must now change to a volt representation transported on the channel. has a binary value '0' and Associated a value between 0.05 and 1 in voltage, and for a bit '1 'a value between -1 and -0.05.

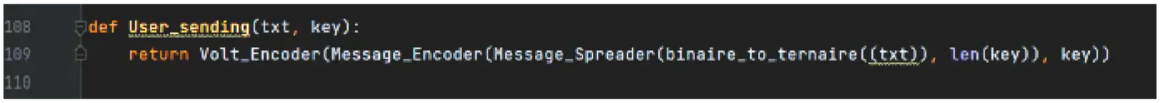
The preparation step is therefore the transition from ASCII value to a voltage representation.



```
def Volt_Encoder(Encoded):
    # Permet de faire le mapping entre une valeur binaire et une plage de volt
    Volt_Encoded = []
    for i in range(len(Encoded)):
        volt = random.uniform(0.05, 1)  # (0.5,1.5)
        if Encoded[i] == 1:
            volt = -volt
        Volt_Encoded.append(volt)
    return Volt_Encoded
```

- ***ASCII:***

The ASCII standard is widely used in computing to encode characters. This name comes from the English acronym "American Standard Code for Information Interchange" which means in French "American Standard Code for the Exchange of Information". [18]



```
def User_sending(txt, key):
    return Volt_Encoder(Message_Encoder(Message_Spreader(binaire_to_ternaire((txt)), len(key)), key))
```

III.6.2.2 Multiplexing:

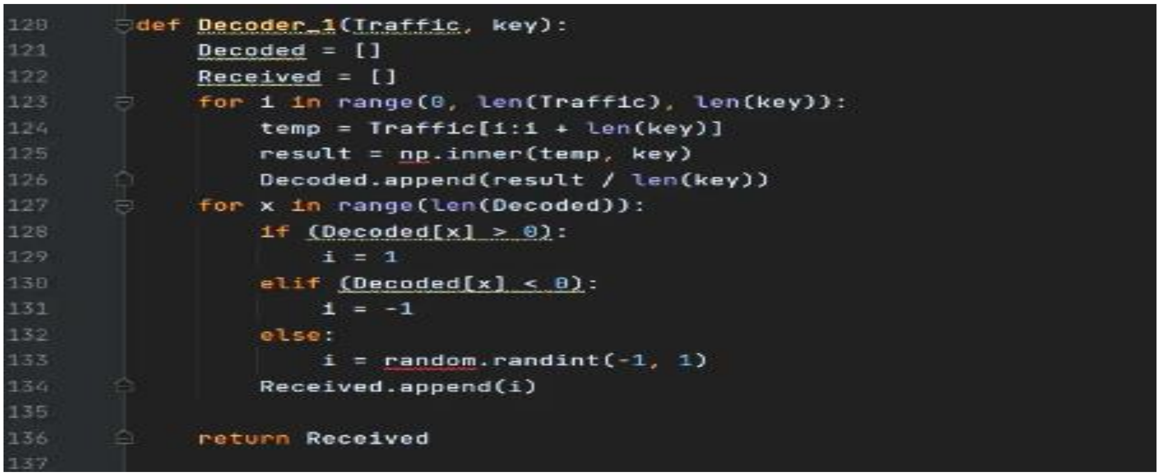
Multiplexing is a way of sending multiple signals or streams of information over a communications link at the same time in the form of a single, complex signal. When the signal reaches its destination, a process called multiplexing recovers the separate signals and outputs them to individual lines. [19]

III.6.2.3 Restitution:

- ***Message decoding :***

The traffic received converted to reconstitute the message of each user.

Decoding is the process of turning communication into thoughts. For example, you may realize you are hungry and encode the following message to send to your roommate: “I'm hungry. Do you want to get pizza tonight?” As your roommate receives the message, they decode your communication and turn it back into thoughts to make meaning.

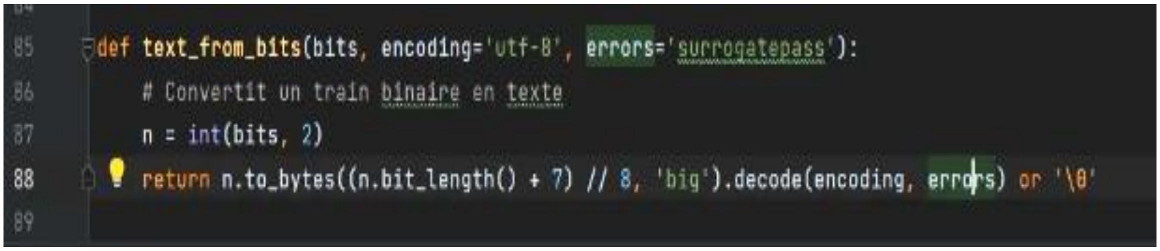


```
def Decoder_1(Traffic, key):
    Decoded = []
    Received = []
    for i in range(0, len(Traffic), len(key)):
        temp = Traffic[i:i + len(key)]
        result = np.inner(temp, key)
        Decoded.append(result / len(key))
    for x in range(len(Decoded)):
        if (Decoded[x] > 0):
            i = 1
        elif (Decoded[x] < 0):
            i = -1
        else:
            i = random.randint(-1, 1)
        Received.append(i)

    return Received
```

- ***Conversion to text :***

At this level the message on receipt and convert to ASCII.



```
def text_from_bits(bits, encoding='utf-8', errors='surrogatepass'):
    # Convertit un train binaire en texte
    n = int(bits, 2)
    return n.to_bytes((n.bit_length() + 7) // 8, 'big').decode(encoding, errors) or '\0'
```

III.6.2.4 Bit error rate calculations:

The bit error rate (BER), or perhaps more appropriately the bit error ratio, is the number of bits received in error divided by the total number of bits transferred. We can estimate the BER by calculating the probability that a bit incorrectly received due to noise. [20]

II.7 Implementation and Results:

In the beginning, we first chose one user with several modulation types, that is, a type within the network, a type outside the network, and an intruder to the network. We first randomly chose the indicator for the specific type of modulation, and then we changed the noise from zero to a hundred and extracted BER each time and so on with the rest of the modulation types.

III.7.1 In the case of a single user:

We chose the indicator in=4131 and modulation type is 8PSK, which is inside the network.

Table III.7: BER measurements in terms of NOISE for a single user of 8PSK

Noise	**3**	**23**	**36**	**45**	**54**	**70**	**84**	**100**
BER	27	48	52	57	62	73	62	57

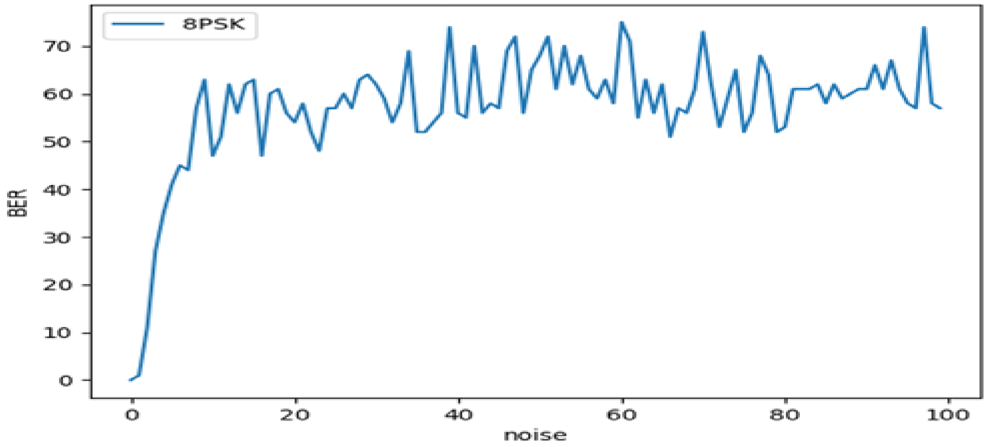


Figure III.15: noise as a function of BER for single user 8PSK modulation.

NB: Bit error rate (BER) as a function of noise (bruit),The figure shows the bit error rate (BER) in the case of a single user (8PSK), the bit error rate is progressively high, meaning the higher the noise, the higher the bit error rate, meaning that the relationship between them is direct.

We chose the indicator in= 112940_and modulation type is GFSK, which is outside the network.

Table III.8: BER measurements in terms of NOISE for a single user of GFSK

Noise	**3**	**23**	**36**	**45**	**54**	**70**	**84**	**100**
BER	20	66	44	58	59	52	62	61

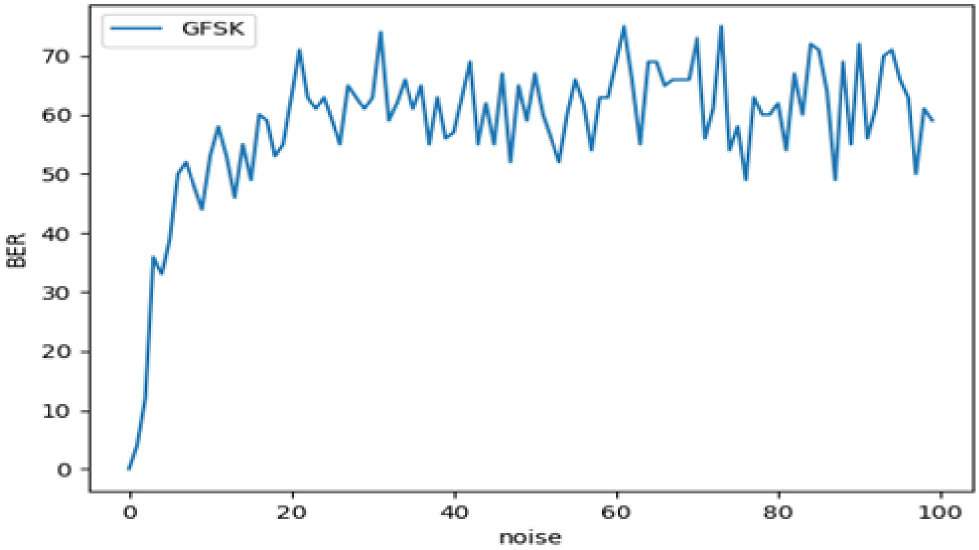


Figure III.16: noise as a function of BER for single user GFSK modulation.

We chose the indicator in= 121546 and modulation type is PAM-4, which is jamming.

Table III.9: BER measurements in terms of noise for a single user of PAM-4

Noise	**3**	**23**	**36**	**45**	**54**	**70**	**84**	**100**
BER	25	61	60	67	62	64	72	65

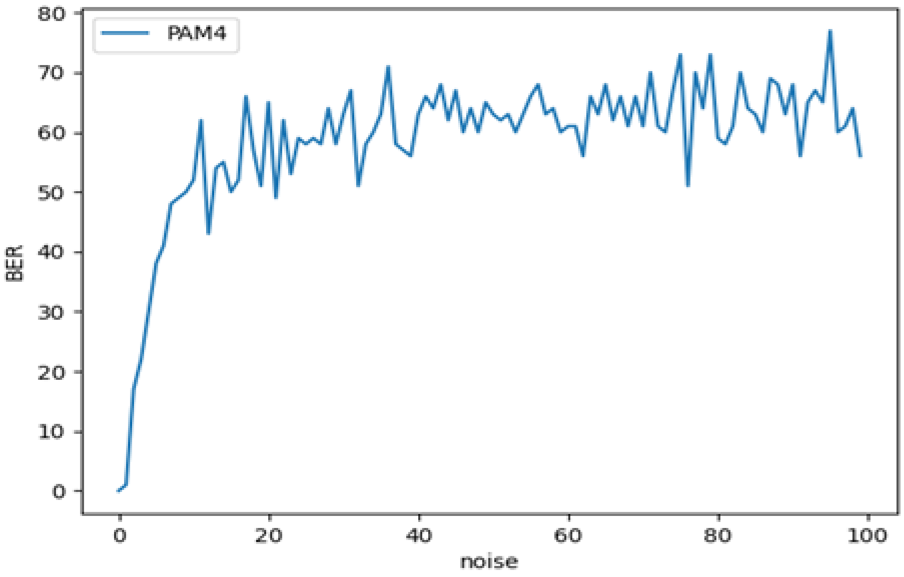


Figure III.17: Noise as a function of BER for single user PAM-4 modulation.

NB: We note that changing the type of user means that if it is (8PSK, GFSK, PAM-4), the bit error rate (BER) compared to noise still high.

III.7.2 In the case of multiple users:

In this step also, we chose five random indicators of each modulation type, that is, we used five users, and then we calculated BER in terms of noise.

We chose the indicator in= {30, 100, 33550, 101760, 149506}_and modulation type is {8PSK BPSK AM-DSB GFSK QAM-16} in the order.

Table III.10: BER measurements in terms of NOISE for a five users (8PSK, BPSK, AM-DSB, GFSK, QAM-16)

	Noise	**10**	**20**	**30**	**40**	**50**	**70**	**80**	**100**
Bit error rate	**8PSK**	22	59	53	63	62	70	60	68
	BPSK	16	57	53	54	68	66	68	69
	AM-DSB	10	55	70	65	57	67	55	60
	GFSK	18	53	61	61	55	56	61	68
	QAM-16	12	53	65	64	66	57	64	64

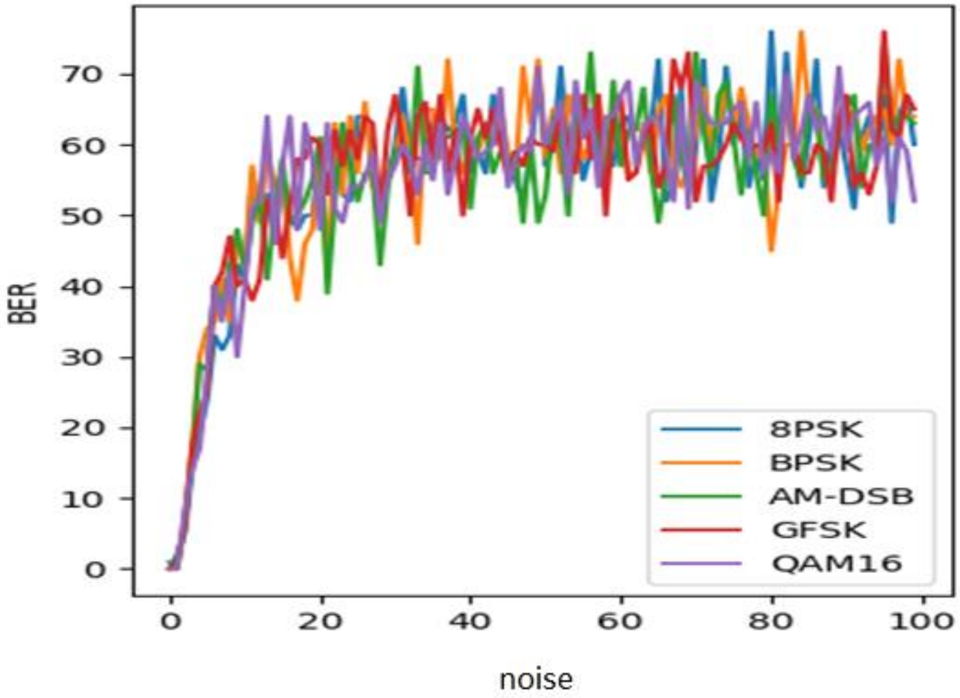


Figure III.18: noise as a function of BER for five users.

NB: Figure III.6 BER as a function of NOISE, We note that the larger the number of users, the higher the BER.

III.7.3 In the case of multiple users with deep learning:

In this last step, we repeated the same as the previous step, but with deep learning.

Table III.11: BER measurements in terms of NOISE for a five users with deep learning (QPSK, CPFSK, AM-SSB, GFSK)

	noise	0	10	20	30	40	50	70	80	100
BER	QPSK	0	51	54	59	66	66	61	59	59
	CPFSK	0	48	53	60	65	51	61	57	59
	AM-SSB	0	46	59	62	58	53	73	59	71
	GFSK	0	39	56	62	61	55	65	53	64

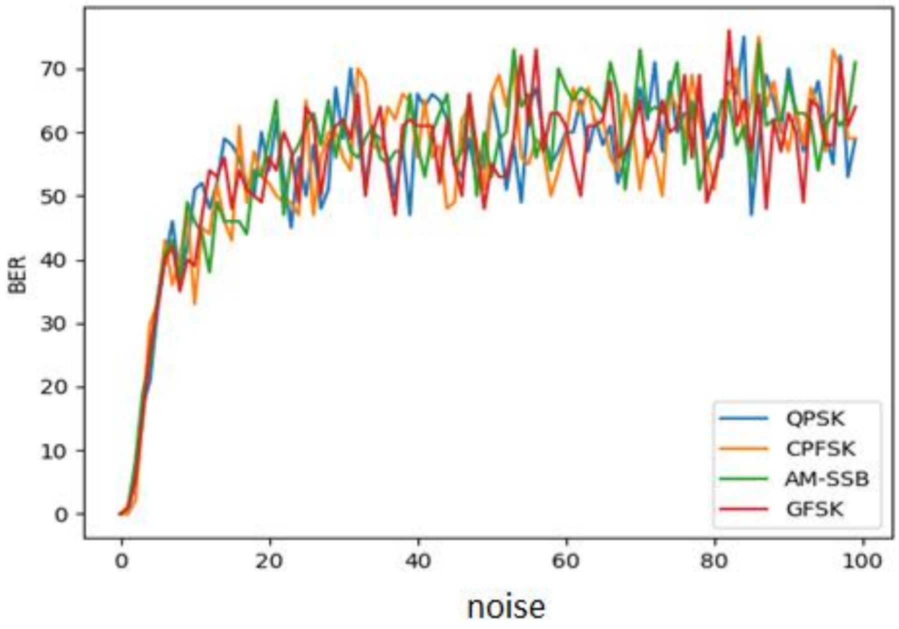


Figure III.19: noise as a function of BER for five users using deep learning.

NB: The same observation as the previous one with regard to the number of users and noise in terms of an error in the bits, but with deep learning, the intruder deleted, meaning that the network does not classify it.

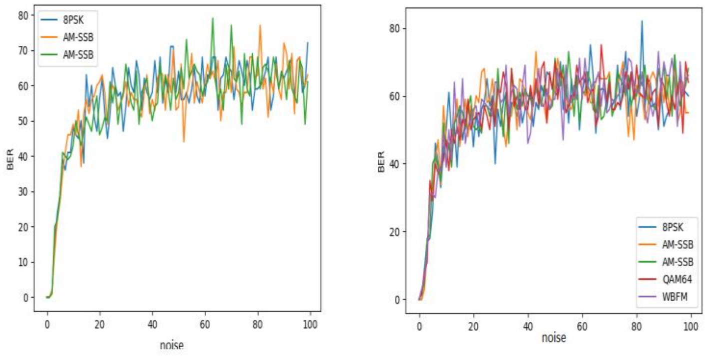
II.7.4 Comparison of Results:

In this part, we compare our results in a stage before using deep learning with our results after using deep learning with the use of the same data.

The following table shows a comparison of the results:

TableIII.12: Compare the results between each other.

	data	Number of users	Noise	results
After deep learning	RML2016.10a_dict	5 users	0 To 100	8PSK,AM-SSB,AM-SSB,QAM-16,WBFM
Before deep learning	RML2016.10a_dict	5 users	0 To 100	8PSK,AM-SSB,AM-SSB



(a) (b)

Figure III.20: noise as a function of BER for five users in (a) after using deep learning and (b) before using deep learning.

II.7.5 Discussions:

In this study, we relied on the results of the first part, which classified the modifications. In the case of a user or several users, the program will automatically classify and when using the same number of users with deep learning, we find that the intruder deletes our results show that noise directly related to BER, especially when noise is increased. The more users compared to the noise, the higher the bit-error rate

III.8 Conclusion:

In this third and final chapter, we introduced the various steps and methods we introduced an optimized deep neural architecture to perform radio signal identification tasks, an important aspect of building the spectrum sensing capability required by software-defined radio. The objective was to achieve feature extraction by learning from the signals of the original samples in the training data set and to evaluate performance on the validation data set in order to predict the intruder.

The results obtained through a single database via CNN algorithm, we have been able to draw the best prediction models.

CDMA measured as an augmented wireless mode and considered a secure 3G fast data transfer and exchange mode. It is now ruling the world by integrating GSM technologies to provide LTE or 4G internet services at full speed.

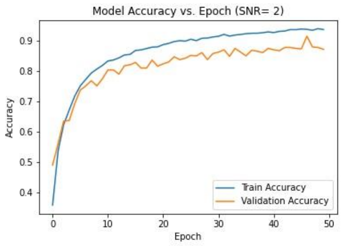
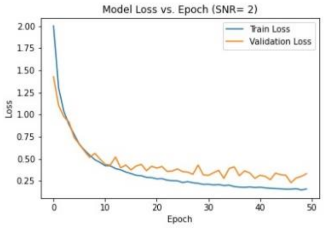
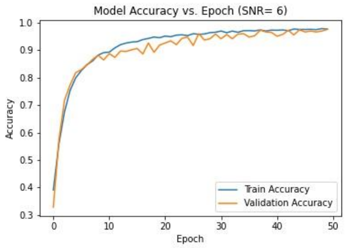
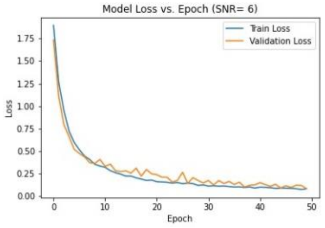
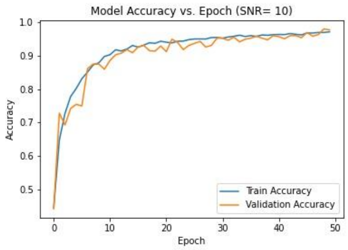
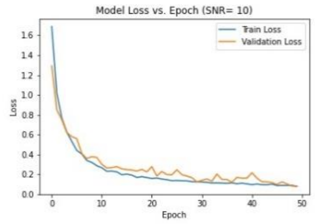
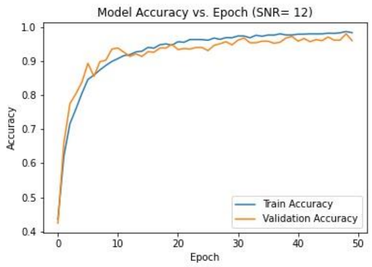
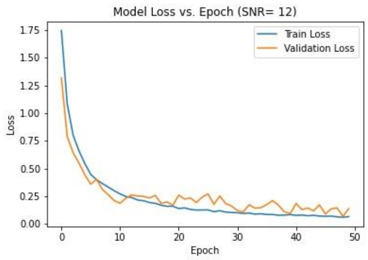
CDMA is a transmission method that allows several different signals to pass through the same channel. However, this process has a negligible bit error rate (BER) but with on-channel noise.

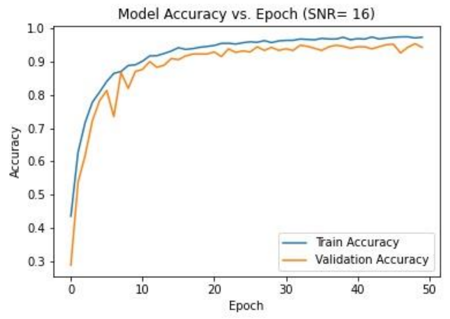
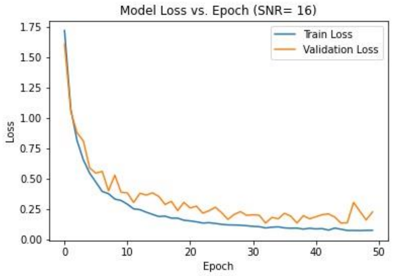
Annexe **A**

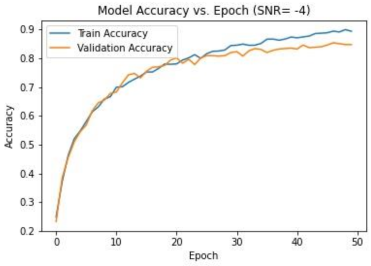
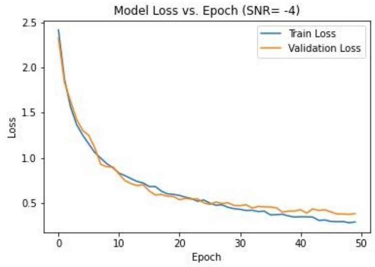
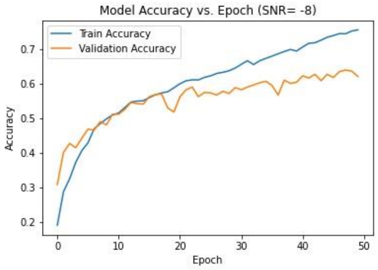
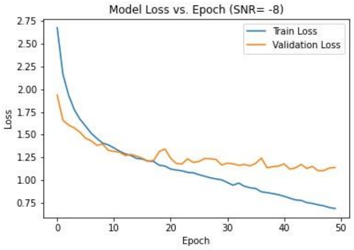
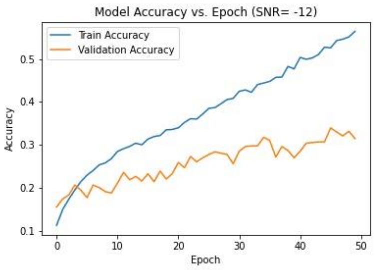
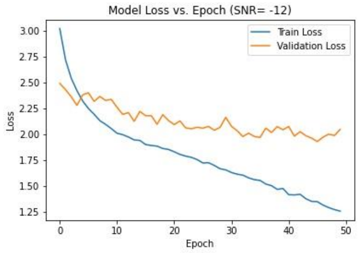
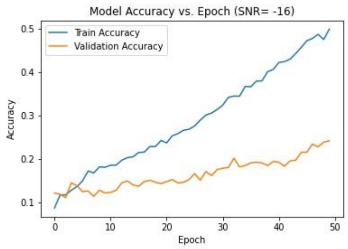
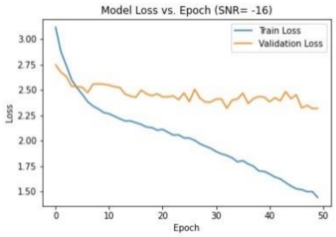
Annex:

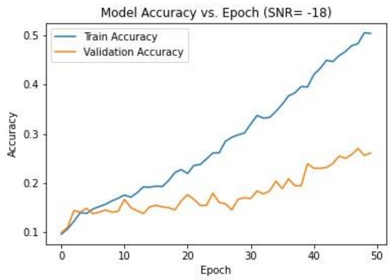
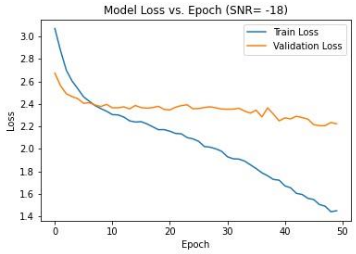
This part will be devoted to presenting the practical work that was not presented in the chapter III

Annex I: Accuracy and Loss

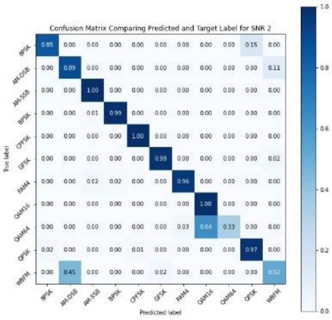
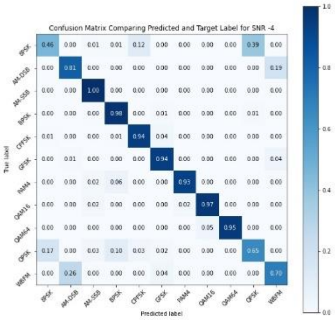
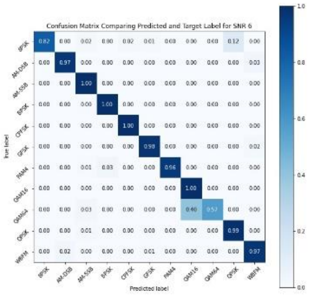
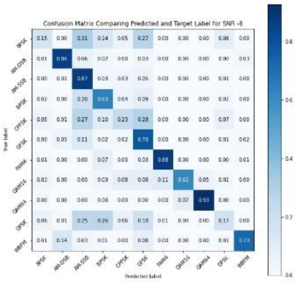
SNR	Accuracy	Loss
SNR=2		
SNR=6		
SNR=10		
SNR=12		

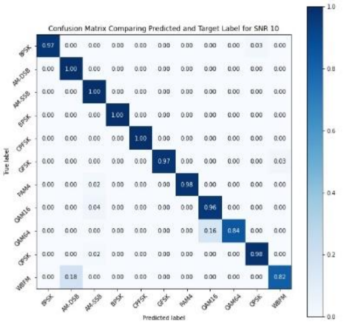
SNR=16		

SNR	**Accuracy**	**Loss**
SNR=-4		
SNR=-8		
SNR=-12		
SNR=-16		

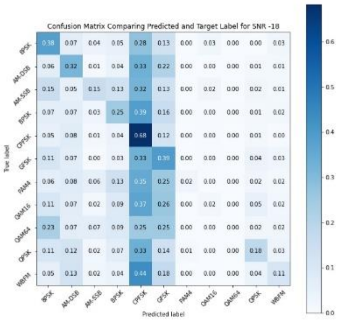
<table>
<tr>
<td><b>SNR=-18</b></td>
<td>
</td>
<td>
</td>
</tr>
</table>

Annex II: Confusion matrix

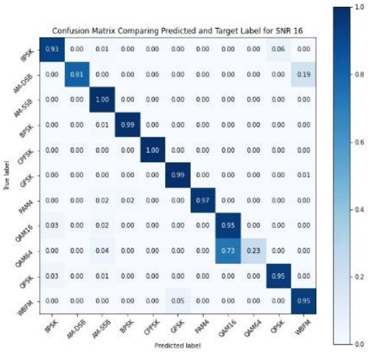
<table>
<tr>
<th>SNR positive</th>
<th>SNR negative</th>
</tr>
<tr>
<td>
</td>
<td>
</td>
</tr>
<tr>
<td>
</td>
<td>
</td>
</tr>
</table>



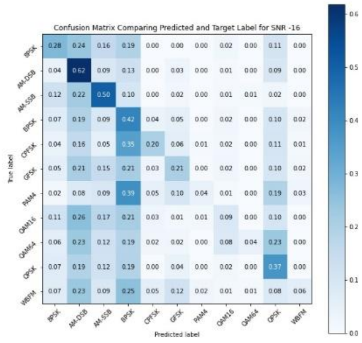
	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.97	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00
AM-DSB	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.97	0.00	0.00	0.00	0.00	0.03
PAM4	0.00	0.00	0.02	0.00	0.00	0.00	0.98	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.04	0.00	0.00	0.00	0.00	0.96	0.00	0.00	0.00
QAM64	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.16	0.84	0.00	0.00
QPSK	0.00	0.00	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.98	0.00
WBFM	0.00	0.18	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.82



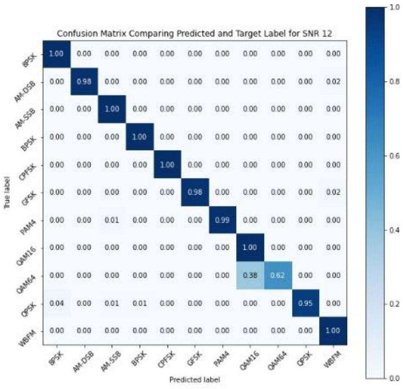
	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.38	0.07	0.04	0.05	0.28	0.13	0.00	0.03	0.00	0.00	0.03
AM-DSB	0.06	0.32	0.01	0.04	0.33	0.22	0.00	0.00	0.00	0.01	0.01
AM-SSB	0.15	0.05	0.15	0.13	0.32	0.13	0.00	0.02	0.00	0.02	0.01
BPSK	0.07	0.07	0.03	0.25	0.39	0.16	0.00	0.00	0.00	0.01	0.02
CPFSK	0.05	0.08	0.01	0.04	0.68	0.12	0.00	0.00	0.00	0.01	0.00
GFSK	0.11	0.07	0.00	0.03	0.33	0.39	0.00	0.00	0.00	0.04	0.03
PAM4	0.06	0.08	0.06	0.13	0.35	0.25	0.02	0.00	0.00	0.02	0.02
QAM16	0.11	0.07	0.02	0.09	0.37	0.26	0.00	0.02	0.00	0.05	0.02
QAM64	0.23	0.07	0.07	0.09	0.25	0.25	0.00	0.00	0.00	0.02	0.02
QPSK	0.11	0.12	0.02	0.07	0.33	0.14	0.01	0.00	0.00	0.18	0.03
WBFM	0.05	0.13	0.02	0.04	0.44	0.18	0.00	0.00	0.00	0.04	0.11



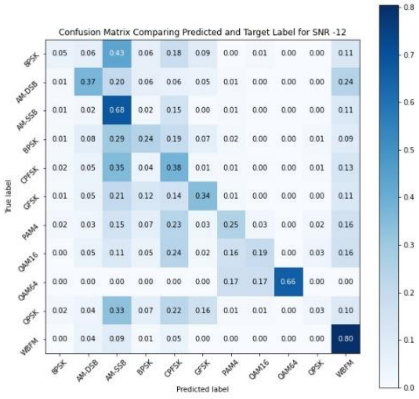
	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.93	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00
AM-DSB	0.00	0.81	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.19
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.01	0.99	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.99	0.00	0.00	0.00	0.00	0.01
PAM4	0.00	0.00	0.02	0.02	0.00	0.00	0.97	0.00	0.00	0.00	0.00
QAM16	0.03	0.00	0.02	0.00	0.00	0.00	0.00	0.95	0.00	0.00	0.00
QAM64	0.00	0.00	0.04	0.00	0.00	0.00	0.00	0.73	0.23	0.00	0.00
QPSK	0.03	0.00	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.95	0.00
WBFM	0.00	0.00	0.00	0.00	0.00	0.05	0.00	0.00	0.00	0.00	0.95



	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.28	0.24	0.16	0.19	0.00	0.00	0.00	0.02	0.00	0.11	0.00
AM-DSB	0.04	0.62	0.09	0.13	0.00	0.03	0.00	0.01	0.00	0.09	0.00
AM-SSB	0.12	0.22	0.50	0.10	0.00	0.02	0.00	0.01	0.01	0.02	0.00
BPSK	0.07	0.19	0.09	0.42	0.04	0.05	0.00	0.02	0.00	0.10	0.02
CPFSK	0.04	0.16	0.05	0.35	0.20	0.06	0.01	0.02	0.00	0.11	0.01
GFSK	0.05	0.21	0.15	0.21	0.03	0.21	0.00	0.02	0.00	0.10	0.02
PAM4	0.02	0.08	0.09	0.39	0.05	0.10	0.04	0.01	0.00	0.19	0.03
QAM16	0.11	0.26	0.17	0.21	0.03	0.01	0.01	0.09	0.00	0.10	0.00
QAM64	0.06	0.23	0.12	0.19	0.02	0.02	0.00	0.08	0.04	0.23	0.00
QPSK	0.07	0.19	0.12	0.19	0.00	0.04	0.00	0.02	0.00	0.37	0.00
WBFM	0.07	0.23	0.09	0.25	0.05	0.12	0.02	0.01	0.01	0.08	0.06



	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
AM-DSB	0.00	0.98	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.02
AM-SSB	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
BPSK	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
CPFSK	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00	0.00	0.00	0.00
GFSK	0.00	0.00	0.00	0.00	0.00	0.98	0.00	0.00	0.00	0.00	0.02
PAM4	0.00	0.00	0.01	0.00	0.00	0.00	0.99	0.00	0.00	0.00	0.00
QAM16	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00	0.00	0.00	0.00
QAM64	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.38	0.62	0.00	0.00
QPSK	0.04	0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.95	0.00
WBFM	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	1.00



	8PSK	AM-DSB	AM-SSB	BPSK	CPFSK	GFSK	PAM4	QAM16	QAM64	QPSK	WBFM
8PSK	0.05	0.06	0.43	0.06	0.18	0.09	0.00	0.01	0.00	0.00	0.11
AM-DSB	0.01	0.37	0.20	0.06	0.06	0.05	0.01	0.00	0.00	0.00	0.24
AM-SSB	0.01	0.02	0.68	0.02	0.15	0.00	0.01	0.00	0.00	0.00	0.11
BPSK	0.01	0.08	0.29	0.24	0.19	0.07	0.02	0.00	0.00	0.01	0.09
CPFSK	0.02	0.05	0.35	0.04	0.38	0.01	0.01	0.00	0.00	0.01	0.13
GFSK	0.01	0.05	0.21	0.12	0.14	0.34	0.01	0.00	0.00	0.00	0.11
PAM4	0.02	0.03	0.15	0.07	0.23	0.03	0.25	0.03	0.00	0.02	0.16
QAM16	0.00	0.05	0.11	0.05	0.24	0.02	0.16	0.19	0.00	0.03	0.16
QAM64	0.00	0.00	0.00	0.00	0.00	0.00	0.17	0.17	0.66	0.00	0.00
QPSK	0.02	0.04	0.33	0.07	0.22	0.16	0.01	0.01	0.00	0.03	0.10
WBFM	0.00	0.04	0.09	0.01	0.05	0.00	0.00	0.00	0.00	0.00	0.80

General Conclusion

The spread of wireless networks has increased in recent times, has become a person has connected to the internet through his device and mobile phone for long hours, which sometimes exposes him to security risks, considering the enormous development in this field and the large number of people who are interested in it.

In this study, systematic efforts made to design a Wireless Network attack prediction system.

This work led us to the development of a data classification study using CNN algorithm applied to the database.

So that in the future, the objective is to give network owners the possibility to apply various CNN techniques in wireless network security. It is clear that the proposed model obtains very promising results in Classification; with the growing demand on network security, the proposed model can be very useful in order to make decisions, because by using such an effective model, they can make decisions that are more accurate. Based on the CNN algorithm, we have developed a modulation classification solution then the use of CDMA technology, which can shorten the delays and send the data securely and confidentially for helping the user.

Reference

Chapter I

1. www.math.univ-toulouse.fr/~besse/Wikistat/pdf/st-m-hdstat-rnn-deep-learning.pdf
2. training.ti.com/sites/default/files/docs/introduction-to-deep-learning.pdf
3. www.researchgate.net/publication/341652370_Deep_Learning_Techniques_An_Overview
4. arxiv.org/pdf/1709.01412.pdf
5. www.googleadservices.com/pagead/aclk
6. ian-goodfellow-yoshua-bengio-aaron-courville-deep-learning-pre-pub-version-mit-press-2016pdf_compress.pdf
7. 9783319944623.pdf
8. alex.smola.org/drafts/thebook.pdf
9. ai.stanford.edu/~Nilsson/MLBOOK.pdf
10. www.cs.huji.ac.il/w~shais/UnderstandingMachineLearning/understanding-machine-learning-theory-algorithms.pdf
11. cs.calvin.edu/courses/cs/344/kvlinden/resources/AIMA-3rd-edition.pdf
12. www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf
13. www.researchgate.net/file.PostFileLoader.html?id=5440e3bdd5a3f298288b45fe&assetKey=AS%3A273625985290242%401442248926315
14. www.pdfdrive.com/artificial-intelligence-for-dummies-e187568767.html
15. www.pdfdrive.com/hands-on-machine-learning-with-scikit-learn-and-tensorflow-concepts-tools-and-techniques-to-build-intelligent-systems-d168440497.html
16. www.pdfdrive.com/introduction-to-machine-learning-with-python-d58337749.html
17. www.expert.ai/blog/machine-learning-definition/
18. www.tutorialspoint.com/machine_learning/machine_learning_tutorial.pdf
19. www.googleadservices.com/pagead/aclku
20. www.pdfdrive.com/fundamentals-of-machine-learning-for-predictive-data-analytics-algorithms-worked-examples-and-case-studies-d178270191.html
21. www.pdfdrive.com/machine-learning-step-by-step-guide-to-implement-machine-learning-algorithms-with-python-d158324853.html
22. www.pdfdrive.com/introduction-to-machine-learning-second-edition-adaptive-computation-and-machine-learning-d162136143.html
23. csc.lsu.edu/~jianhua/csc7333-intro-0.pdf
24. www.pdfdrive.com/deep-learning-adaptive-computation-and-machine-learning-d176370174.html
25. hunterheidenreich.com/blog/breaking_down_ml_for_the_average_person/
26. www.guru99.com/reinforcement-learning-tutorial.html
27. vitalflux.com/reinforcement-learning-real-world-examples/
28. www.pdfdrive.com/pro-machine-learning-algorithms-a-hands-on-approach-toimplementing-algorithms-in-python-and-r-d196902175.html

29. www.pdfdrive.com/machine-learning-an-algorithmic-perspective-2nd-edition-d60539459.html
30. www.researchgate.net/publication/303806260_Machine_Learning_Algorithms_and_Applications
31. datageneralist.files.wordpress.com/2018/03/master_machine_learning_algo_from_scratch.pdf
32. www.simplilearn.com/10-algorithms-machine-learning-engineers-need-to-know-article
33. www.pdfdrive.com/introduction-to-deep-learning-using-r-a-step-by-step-guide-to-learning-and-implementing-deep-learning-models-using-r-d158252417.html
34. www.pdfdrive.com/learn-keras-for-deep-neural-networks-a-fast-track-approch-to-modern-deep-learning-with-python-d185770502.html
35. hagan.okstate.edu/NNDesign.pdf
36. www.simplilearn.com/tutorials/deep-learning-tutorial/introduction-to-deep-learning
37. news.microsoft.com/wp-content/uploads/prod/sites/93/2020/04/Student-Guide-Module-4-Deep-Learning-and-Neural-Networks.pdf
38. www.simplilearn.com/tutorials/deep-learning-tutorial/deep-learning-applications
39. ijeast.com/papers/310-316,Tesma412,IJEAST.pdf

Chapter II

1. HEDNA Saida, « Gestion de l'économie d'énergie dans les réseaux sans fil 802.11 Ad Hoc » ; Mémoire de Magister, Université de Université El Hadj Lakhdar – BATNA 2006 /2007.
2. Les réseaux sans fil (Wireless Networks), HADDACHE © 2010/2011
3. DI GALLO Frédéric**, «** Wifi L'essentiel qu'il faut savoir… », Extraits de source diverses récoltées en 2003.
4. ABOURA Wissam, BENHABIB Iman, « Etude et caractérisation de la couche physique dustandard) IEEE802.16/WIMAX (», Mémoire de Master, UniversitéAbouBekrBelkaid, Tlemcen, Faculté de Technologie, 2010.
5. BELABDELLI Abdelheq, OUKAZ Mokhtar, « Dimensionnement D'un Réseau Sans Fil Wifi », Mémoire de Master, Mémoire de Master, Université AbouBekr Belkaid, Tlemcen, Faculté de Technologie, 2012.
6. http://fr.wikipedia.org/wiki/General_Packet_Radio_Service.
7. memoireonline.com/07/08/1383/m_u-m-t-s21.html
8. Wireless_Network_Security_Vulnerabilities_Threats_and_Countermeasures_IJMUE_vol2_no2.pdf.
9. academia.edu/22127644/Wireless_Security_Wireless_Security_Types_of_Security
10. ummto.dz/dspace/bitstream/handle/ummto/8253/BoubekeurKarima
11. ummto.dz/dspace/handle/ummto/6244

Chapter III

1. www.tutorialspoint.com/cdma/cdma_technology.htm)
2. www.dominodatalab.com/data-science-dictionary/anaconda
3. dzone.com/articles/python-anaconda-tutorial-everything-you-need-to-kn
4. www.datacamp.com/community/tutorials/tutorial-jupyter-notebook
5. santebf.net/formations/python/
6. www.python-simple.com/python-pandas/panda-intro.php
7. www.hebergementwebs.com/nouvelles/top-10-des-bibliotheques-de-science-des-donnees-en-python
8. www.geeksforgeeks.org/introduction-to-pandas-in-python/
9. www.ques10.com/p/47055/compare-dsb-fc-dsb-sc-and-ssb-sc/
10. www.learnbywatch.com/wide-band-frequency-modulation-wbfm/
11. www.academia.edu/37115041/DIGITAL_MODULATION
12. sites.google.com/site/near communications/gfsk-modulation
13. .carrier.huawei.com/~/media/CNBGV2/download/products/networks/50G-PAM4-Technical-White-Paper.pdf
14. https://deepai.org/publication/deep-learning-for-rf-signal-classification-in-unknown-and-dynamic-spectrum-environments
15. https://www.iith.ac.in/~tbr/teaching/docs/DigitalModulation-WhitePaper.pdf
16. cse.iitd.ac.in/~cs1120231/Walsh
17. ecampusontario.pressbooks.pub/commbusprofcdn.
18. glossaire.infowebmaster.fr/ascii/
19. techtarget.com/searchnetworking/definition/multiplexing
20. web.mit.edu/6.02/www/s2011/handouts/L07_slides.
21. http://noiselab.ucsd.edu/ECE228-2020/projects/Report/76Report.pdf.