National College of Ireland

Analysis and Detection of Unauthorized Access Points Using various Machine Learning Algorithms.

MSc Internship
Cyber Security

Akshay Mangesh Juwale
Student ID: X19129866

School of Computing
National College of Ireland

Supervisor: Prof. Niall Heffernan

National College of Ireland
Project Submission Sheet
School of Computing

National College of Ireland

Student Name:	Akshay Mangesh Juwale
Student ID:	X19129866
Programme:	Cyber Security
Year:	2020
Module:	MSc Internship
Supervisor:	Prof. Niall Heffernan
Submission Due Date:	17/08/2020
Project Title:	Analysis and Detection of Unauthorized Access Points Using various Machine Learning Algorithms.
Word Count:	4912
Page Count:	13

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:	Akshay Mangesh Juwale
Date:	17th August 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Analysis and Detection of Unauthorized Access Points Using various Machine Learning Algorithms.

Akshay Mangesh Juwale
X19129866

Abstract

Illegal access points in an internet network is a frequent concern for users connected to the network, in this paper, we try to identify the illegal access point entries via RTT Round Trip Time data gathered through all the nodes connected to the network. We will apply machine learning models, in order to correctly classify the access points as authenticated or unauthenticated. Our main objective, in this paper is to study the effectiveness of identification of various illegal access points through various machine learning algorithms such as SVM Support vector machines, KNN K means the nearest neighbour and Genetic algorithms. On performing a comparative analysis among multiple algorithms, we have found that Ant colony Optimization algorithm achieves the highest accuracy of 98.15%. In the proposed work, the synthetic RTT dataset has been generated using network simulation for performing predictive analysis.
Keywords – Illegal Access point, Machine learning, genetic algorithm, network protection.

1 Introduction

The devices known as wireless access points are linked to a company's network system through a computer. The computer network permits wireless kind of devices, for example, the laptops which are used by an employee for being able to join the network system without the help of a limiting "physical network cable". Wireless networking systems are considered as the most workable way to provide organisational resources to the employees for great working experience for many companies. However, there is a grave drawback of these access points. These are more vulnerable to be accessed by unauthorised users due to its 24/7 availability in the connection. This study has been conducted to develop algorithms using "Genetic", "SVM", "KNN" for the purpose of detecting unauthorised access. This chapter has included the background of the research, the aims, objectives. Research rationale and questions have been formed that would guide the research. The research significance would help to understand the contribution of this research study in the detection of unauthorised access to wireless networking systems. Moreover, the research framework has been formed for better conceptual understanding for the readers. The conclusion of this chapter would help to understand the research plan and design as a summarised way.

As the sheer number of "applications" that are using wireless networking systems, in which some of these are crucial in nature for some users and employees, enterprises. That

is why effective management in wireless networking is necessary. Therefore, openness, as well as availability for all time of these wireless network systems, are becoming top priorities, creating it an elementary resource to be effectively managed [1]. Hence, many employees, students, enterprises are accessing various wireless networks, of which the access points do not have enough security in accessing. Moreover, the traffic which is carried by them is not actually encrypted [2]. As a result, the sensitive data and communications, transactional processes of the users are highly falling into vulnerable condition as these could be hacked or accessed by any illegal authorisation. This would make the users fall into a great risky situation. Such risky incidents take place as the connection of the users is being remitted "In the Clear", the sniffing tools could be used by the actors who are malicious. The main objective of accessing the tools by these malicious actors are to access or for obtaining the information which is sensitive in nature, for example, "passwords" of various important accounts, "credit card numbers". Without security, the wireless networking systems used by the public consisted of "unsecured file sharing", that could permit an illegal user to grasp any sort of files and directories that might be available unintentionally for sharing purpose by a user. The other risks which can take place due to the wireless networking system are "Piggybacking", " wireless sniffing", "evil twin attacks", "wardriving", " shoulder surfing". As various anomalies such as "volume-based", "spatial-based" derived from different sources might arise at the indifferent time in a realistic scenario of the wireless network [3]. Making the detection of the various anomalies by using or applying "profile-based solutions" with the help of "single dimension metrics" is not considered as an ideal or efficient measure. For instance, selecting "volume-based attributes", such as the digit of the bits, flows and various packets, while making use of "spatial-based attributes" [4]. The attributes based on spatial are including the source as well as destinations related to IP-addresses and ports. As in the case of a former, though, they are able to match the primary behaviours of "DDoS attacks", "flash crowds", such attributes have the difficulty of to detect the unauthorised access. With the goal of solving the restrictions of the approach which are signature-based, a wide number of "profile-based" approaches have been introduced. Due to the flexible features and necessity to support the wireless network management, the used methods of these proposed approaches do vary in denomination, such as statistical approach, clustering process, the process of soft computing. Chen and Ye founded a theory which is known as "Chisquare theory" for the purpose of anomaly identification as well as unauthorised access detection. According to previous studies associated with the detection of illegal access, various approaches have been proposed. "Daedalus' ' a detection of anomalies based on time series or statistical approaches that help to address many limitations and can capture the behaviour as well as network prole from "BRO NIDS connection logs". Some machine learnings have been proposed to predict the "normal trac behaviour" and to remove uncertainties and sounds by applying "Particle Swarm Optimization" (Ling and Wu, 2019). The application of PSO consisted of the "Stationarity Dickey-Fuller" test. Moreover, the scores had been computed with the help of "Fuzzy Logic" for dealing with vagueness. SVM or "Support Vector Machine", KNN or "K-nearest neighbour" and "Genetic algorithm" are some popular approaches which have been discussed in the study by exploring the working strategies, effectiveness, accuracy level as well, in the detection of illegal accesses to the wireless networking systems. The "RTT or Round Trip Time" value dataset of the points of access of the wireless networks have been used. Also, the mentioned machine learnings have been applied to the data series for analysing whether the points for accessing are unauthorised or authorised in

nature [5]. In a wireless network, an access point is regarded as a way of transmitting and receiving data and files. These access points are worked to connect the users among each other within the networking system and deliver as a point of interconnection with a network based on a fixed line or in other words a network which is weird. These access points in a wireless networking system are also known as "transceivers". The term "transceivers" is called because of the nature of "transmission" as well as "reception" of these access points in a wireless networking system [6] Because of the usage and existence of many smart devices in this modern era, illegal access points are usual places and could not be avoidable. There are no policies and regulations on the connection lines of such access points on a bare networking system or a network that is secured with authorised users being accessed as a relay. These relays are intended to provide weaker points to the wireless networking system. The network can be damaged via stealing of the information and data directly related to the user and sniffing other information in traffic of the network. With the information which is stolen the networking system and the users who are connected can be damaged or harmed further. Apart from this study, many other studies associated with the risks of wireless networking systems are being conducted progressively by many organisations and researchers currently for addressing the same issue related to this topic. "Support Vector Machine" or SVM is one of the most strong "supervised learning algorithms" in the area of "Gene Expression analysis" and its efficiency in detection of illegal access is trying to be explored through this present study along with the other algorithms namely "KNN", "Genetic algorithms". According to previous studies conducted by Lee [**?**], the approach of "SVM" classification that is well-performing in nature might suffer from consumption that is based on high time or duration, "High CPU", and "physical memory usages" because of providing intricate training and the classifying method, especially in the case of a high dimensional dataset.

1.1 Research Objective

The critical aspects of the study can be defined using the objectives, which are:

- To explore the efficiency of different algorithms such as the "SVM (Support Vector Machine), KNN (K-means Nearest Neighbour) and Genetic Algorithms" in detecting "unauthorised access points" within the wireless networks
- To compare the effectiveness of "Genetic Algorithms over SVM and KNN" in the "detection of unauthorised access points."

1.2 Research Question

The research questions would not only guide the study but also would help to determine what the power of this current study is. They are the following:

- In which way the different algorithms which are "genetic algorithms", "SVM or Support Vector Machine", "KNN or k- Nearest Neighbour" are working efficiently in detecting the unauthorised access points in the system of wireless networking?
- Do "Genetic Algorithms" have better competency than the "KNN" and "SVM" in unauthorised access identification?

1.3 Conclusion

This chapter of introduction has included the insights of this current research in a detailed manner. What is the background of the study, what approaches have been proposed by previous studies by many authors related to illegal access to various wireless networking systems. Why this subject has been selected also has been discussed in the research rationale section and the research significance section. It has been discussed overall in this chapter why the access to the wireless network is being a factor of creating risk situations for the users. The aspects of other measures in terms of machine learning and other preventive approaches which have been proposed by other authors also have been discussed in this context, which will allow the reader a better understanding of the overview and background behind the current research study. The research aim, objectives, and research questions have been formed in this chapter for a better approach to pursue the current study as well as enabling the reader to understand the research framework for addressing the result in a significant manner.

2 Literature Review

The research-based on the detecting intruders in the wireless networks using the algorithms can be elaborately conducted with the help of gathering information about the concerned issue and produce genuine evidence from the practical evaluations and researches of eminent persons. The empirical literature sources are a great source of identifying the problems areas of the research that have been conducted on similar areas of the study or on the key aspects of this study. The study of literary sources will highlight the drawbacks and possible areas of improvements that can be utilised to proceed with the current research. Hence, this chapter shall discuss the critical aspects of the research based on the literature presented by other authors in the empirical study and also provide an insight into the lacking areas of the corresponding research studies through the literature gap. Furthermore, the chapter will emphasise on the theories and models corresponding to the application of the algorithms that are used for the purpose of detecting the “illegal access” of intruders in the “wireless networks”. The conceptual framework is also depicted in the chapter with a detailed evaluation of the “dependent and the independent variables” that are essential for the study.

2.1 Detecting Unauthorised Access Points in Wireless Networks

There has been extensive research regarding the detection of the vulnerable points of access in the wireless networks by different authors. One such research is conducted by the authors, Alotaibi and Elleithy, 2016 which elaborates on the concept of “Rogue Access Points (RAP)” that are required to be detected due to the growing concern regarding the increasing security problems of the Wireless LAN that are widely deployed in various sectors of business. The authors have focused their study on the existence of RAP and have presented ways of detecting different types of RAPs such as the “Evil-twin, Unauthorized, Compromised, Improperly Configured RAPs, and Denial of Service RAPs”. The authors have elaborated on the existing vulnerabilities that have not been investigated by other researchers and also identified the detection techniques corresponding to each of the categories of RAPs. The taxonomy behind the RAP classifications has been demonstrated using the state diagrams that define the ”deauthentication/disassociation

attacks" that can be forged by the "legitimate AP to disconnect the users". The authors have discussed the attacks based on their features and their activities in the network. The research has also provided solutions and techniques for handling the security issues at RAPs with the demonstration of the countermeasures that can be employed for the detections and preventions of the attacks. The study also elaborates the various detection approaches such as the "coexistence approaches, approaches handling the evil twin attacks, unauthorised AP countermeasures, deauthentication/disassociation countermeasures" and countermeasures that are capable of solving multiple attacks.

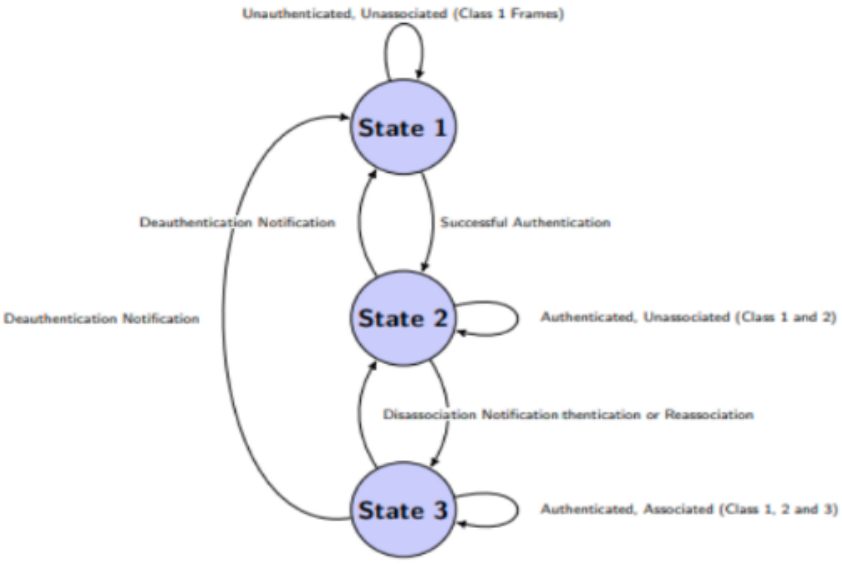

Figure 1: State Diagram for the de-authentication/disassociation attacks

Khan and their team [7] have discussed the vulnerable points of the ad-hoc networks and the detection of the intrusions. The authors have explained the various taxonomy related to the "intrusion detection system" corresponding to the unauthorised access and security attacks. The IDS schemes and approaches have been demonstrated in the paper which have been further elaborated based on the various parameters. The authors have defined the mechanism of detection, which involves the "data collection, data pre-processing, intrusion recognition, intrusion model, reporting and response". The taxonomic classification of the IDS includes the "detection based IDS, signature-based IDS, Anomaly Based and Hybrid". However, each of the detection systems has certain advantages and disadvantages, as mentioned in the journal.

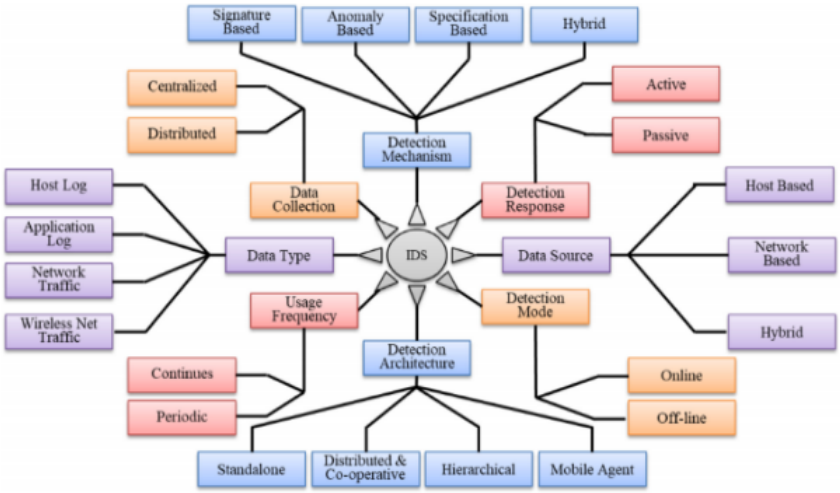

Figure 2: Taxonomy of IDS

The detection modes, responses and architectures corresponding to the detection of intrusions have been elaborated by the authors [7] in their journal. The authors have also classified the several methods and techniques of detection into four major mechanisms which are further sub-classified into techniques of detection. From the journal, it can be observed that "the genetic algorithm" is classified as a "Heuristic Technique" while SVM and KNN are a "Rule Techniques".

2.2 Effectiveness of SVM Algorithm

Authors Reddy [8] have demonstrated the effectiveness of using SVM as the technique of detection unauthorised intrusions highlighting the role of discrimination function. The data mining approach of SVM technique is utilised in this research. The researchers have suggested that the "discriminant function" in SVM technique can effectively help to detect the unauthorised access by identifying the normal and the anomalous activities in the network and separate them to create a response mechanism to avoid the attacks. However, the authors have also indicated that the discriminant function corresponding to the use of SVM technique should be critically chosen to derive the best outcome in the process of detecting "unauthorised access points". It is also provided in the journal that the effectiveness of the SVM technique is based on the "kernel parameters and the classification accuracy of the feature selection". The journal has explored the significant uses of both the linear and non-linear SVM. This technique is also based on the development of the appropriate scaling method, which improved the discriminant function and has enabled the IDS with enhanced efficiency.
The literature presented by Asiegbu et al. 2019 has also supported the effectiveness of the SVM technique in the detection mechanism of "unauthorised access points in a network". The journal has evaluated the efficiency based on the application of SVM on a dataset consisting of 10000 access points, among which 2000 access points were used to evaluate the efficiency of the algorithm. 374 vulnerable access points were identified, and the rate of data misclassification was negligibly indicated by the reduced rate of "false alarms" and high "detection accuracy" of 99.98%. Thus, the authors have demonstrated the effectiveness of the SVM technique in the process of detection

2.3 Effectiveness of KNN Algorithm

The efficiency and performance of the KNN algorithm in the "Intrusion Detection System" are discussed in the journal presented by [9]. The study is based on the "randomisable filtered and K Nearest Neighbor classifier for selecting features" which can enhance the performance of detecting the unauthorised access into the network and also provide improved accuracy to the detection system. The authors have stated that this method is considered to be one of the most simple algorithms that can be used for the purpose of the detection of intrusion. The analytical traceability and traceable behaviour improve anomaly detection. However, the authors have also mentioned the limitations of KNN due to the high storage requirement and are highly "prone to the curse of dimensionality and low rate in classifying test tuples". The experimental analysis that has been provided in the study have indicated that the rate of accuracy of threat detection in access points are quite high for the "normal, probe and Denial of Service attacks" while it is comparatively low in "User to Root" and "Remote to Local" attacks. However, the study has also shown that the outcomes of accuracy and scalability are improved when the "randomisable filter classifier" is used along with the KNN algorithm.
Similar to the objectives of this journal, the authors Shapoorifard and Shamsinejad, 2017 have presented a study that emphasises on the use of KNN is an effective algorithm for the IDS. Being slightly different from the previous journal, this journal has used a hybrid algorithm that used the nearest neighbour technique, farthest neighbour technique and the second nearest neighbour technique to solve the detection of access points in the utilised data set. The results of the technique have shown an extensive level of efficiency and performance in the detection of the intrusions.

2.4 Effectiveness of Genetic Algorithm

According to the authors [10], the Genetic Algorithm can provide the "best detection rate", but this technique also has "the highest false-positive rate" that can lead to low accuracy of "anomaly detection system". Author [11] have used the Genetic Algorithm Approach for the feature selection method in combination with the SVM technique for the detection of the intrusions. The authors have highlighted the use of Genetic algorithms in the feature selection process based on Darwin's principle of natural selection and genetic amplification. The study has also provided an insight into the process of splitting the properties into two features. The data classification methods have effectively reduced the intrusion network data and have provided the basis of the accuracy of data classification. The proposed method of classification and Intrusion detection is highly efficient at selecting a subset based on Genetic algorithm. The two feature selection based on Genetic Algorithm has provided a high rate of accuracy as well as the high rate of precision.

2.5 Literature Gap

The review of literature has provided an overview of the concept development regarding the existing security issues of the network access points. The empirical study of the journal presented by the authors [5] indicates several drawbacks that shall be addressed in further studies. The techniques that have been discussed based on the detection of RAPs have several discrepancies and inadequacies, which can be explained by the "wired side solution" that is presented in the study. This solution uses the "switch port mapping". However, the technique fails to incorporate an "integral authorisation method". Also,

the techniques that have been discussed are not efficient in detecting "RAPs attached to a legitimate AP". Therefore, the development of detecting solutions involves approaches that have unnecessary traffic and increased complexity. The approaches used by the authors broadly rely on "higher-layer protocols that delay the process of detection" and are also dependent on "easily spoofed identifiers such as IP addresses". These areas need to be improved in further research through the appropriate use of algorithms.
There are several challenges to the adoption of the proposed detection systems in the ad-hoc networks as mentioned in the journal presented by Khan et al. 2020 which are the "lack of a central management system, dynamic topology, limited bandwidth, lack of well-defined boundary and lack of power source". Therefore, a detection mechanism has to be developed that does not have these limitations to the system of detecting "unauthorised access". The journal presented by [8] has used the SVM technique for the IDS. However, the technique employed in the research involved the rough set approach, which significantly reduced the detection time. Also, the scaling technique and rough set were individually employed in the research, which has reduced the efficiency of the SVM technique. Therefore, it can be understood that combining scaling and rough set will improve the efficiency of the IDS using SVM.

3 Research Methodology

The proposed methodology has been used in order to correctly classify the unauthorised access point. The overall operation has been performed in many steps. Each step used for proposed model will be explained in upcoming subsections. The Flow Diagram of proposed architecture is shown in Figure 3.

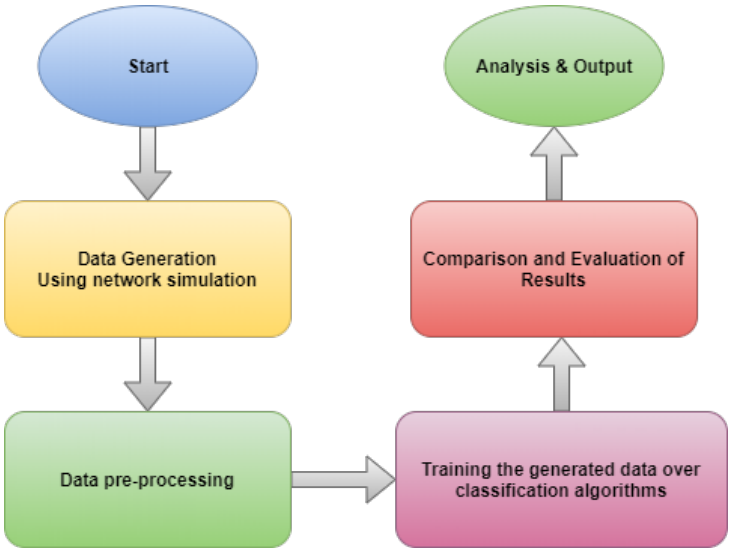

Figure 3: Proposed Architecture

3.1 Data Generation

The real time of network access point is not available publicly. Therefore, we have a generated a synthetic data using network simulation. The generated access point data will be mainly based on the connection type and connection type will has been classified

into 3 categories 3G, 4G and Wired data. For each connection type we will generate a separate data and perform a classification over it. The generated data will have 2 features response time of network and the length of the data packet. These both the features will be used to perform the predictive analysis.

3.2 Data Pre-Processing

The data generated from simulation script will be in raw format. To convert this into the machine readable format, we have to perform some pre-processing steps. The unnecessary string values has been been removed. Only the useful information of network data has been kept for our analysis. After performing data pre-processing there only numerical features available in the dataset.

3.3 Training the Models

After performing the pre-processing on synthetically generated data, now the data will be training using different classification models in order to do a comparative analysis. The classification algorithm used for this analysis are SVM (Support Vector Machine), KNN (K-nearest neighbour) and Ant colony optimization algorithm. SVM and KNN algorithms are the supervised machine learning approaches. Whereas, ant colony optimization technique is genetic algorithm technique. The generated data for different network type will be trained by the model to carryout the predictive examination.

3.4 Evaluation

There are two different approaches will be used for evaluation of each model. First the accuracy of each model will be calculated. later, the precision score will be calculated, in order to check for false positive values. This experiment will be performed over 1000 and 10000 different number of samples. the different subsets of dataset are used in order to find out the impact on increasing the training data. The Evaluation has been carried out by performing iterative operation with algorithm over the same data-set, in order to fine-tune the parameters.

4 Design Specification

The overall design of the proposed framework can be divided into two parts. Simulation design and algorithmic design. In simulation design part, we will discuss about the network simulation part used for data generation. In the algorithmic section design part we will discuss about the design and architecture part of each algorithm.

4.1 Simulation

A simulation program has been designed to simulate a network ping times of all the nodes connected. When the simulation program is run the data for 3G, LTE and Wired would be generated. A simplified form used to feed to ML programs would also be generated. The user has to supply the number of noes and the percentage of exposed nodes in the program and the program would generate the same.

4.2 Algorithmic Design

In our proposed design, we are using 3 different model from algorithmic point of view. Support Vector machine (SVM), K-nearest neighbour (KNN) and Ant colony optimization algorithm. A support vector machine is supervised machine learning (ML) model using classification algorithms. They are used on two group classification problems. The Support vector machine uses the concept of support vectors, to find out the optimal hyperplane. For a optimal hyperplane the maximum margin is required between the support vectors. SVM is all about finding out the best hyperplane for optimal classification.

KNN is a type of map learning algorithm, it maps the input data in space and clusters them into groups based on the nearest possible lengths between two nodes. And groups nearest nodes together to form clusters. So, any new data point mapped to the space would be added to the cluster that it is mapped in that space. The input consists of training data which are grouped with k number of groups in the space they are mapped into. If used for classification purposes the new item is the object assigned to the most common item among any of the kth group and classified by majority vote.

In Ant Colony Optimization (ACO) a set of software agents search for the best possible solution to a given optimization problem. The optimization problem is transformed into finding the best path on a weighted graph where all the inputs are plotted in the graph space. The ants or agents in this model build solution by moving on the graph. The solution there by derived from this algorithm is stochastic and is based on pheromone model. Each ant while traversing through the graph sets a pheromone maker on the place it has visited, and the pheromone degrades based on the time passing. So, the ant visiting the node would identify the marker set by the pervious ant and identify the node is already visited node and would optimize accordingly.

5 Implementation

For the whole analysis purpose, we have used the windows operating system, running on i5 processor with 8 GB of RAM and 512 GB of hard drive. The generated python program can run on any platform by installation of python and the results thus obtained would be similar in comparison results. There are multuple python libraries have been used for our implementation, which includes matplotlib, sklearn, numpy and pandas. The steps of implementation are briefly listed as follows

- Extracting details from raw file and converting it to more readable format
- Reading the file using pandas.read_csv.
- Dividing the data set in train test. Training data for developing the model and Test data for checking/validating model
- Fitting the model
- Test for accuracy and precision of model

In the above implementation, the main objective is to accurately perform the binary classification between unauthorized and authorized access in the network. In the evaluation section, we will discuss about the results achieved for following implementation.

6 Evaluation

The obtained results using all the 3 algorithm will be analyzed and evaluated based on the performance of each model in terms of various metrics. The metrics includes accuracy and precision score.

6.1 Experiment 1/ Accuracy Comparison

The accuracy comparison between Support vector machine, K-nearest neighbour and Ant Colony optimization has been performed for 1,000 and 10,000 number of data samples. We can analyze the accuracy for both the data samples using the graph shown in Figure 4. The Highest accuracy for both the subsets of data have been achieved using ACO (Ant Colony optimization). Also we have observed that, after increasing the size of data accuracy for KNN and ACO algorithm increases. The lowest accuracy have been achieved using Support Vector machine algorithm.

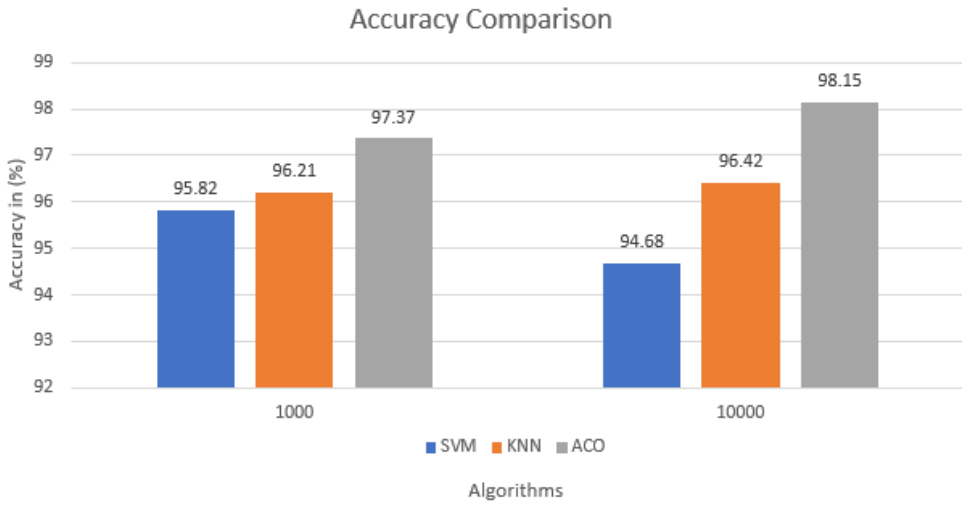

Figure 4: Accuracy Comparison between the algorithms

6.2 Experiment 2/ Precision score Comparison

The precision score has been calculated on the different subset of data using proposed algorithms. The result of precision value is shown in Figure 5. The highest precision score have been achieved is 0.97 using SVM and ACO algorithm. The precision score is mainly calculated to check for false positive values in the dataset. The lowest precision has been achieved using K-nearest neighbour algorithm.

6.3 Discussion

In order to detect the illegal access point, all the proposed model provides the fair accuracy. On comparative analysis we have found that Ant colony optimization algorithm, which is a genetic algorithm provides the better accuracy and precision rate as compared

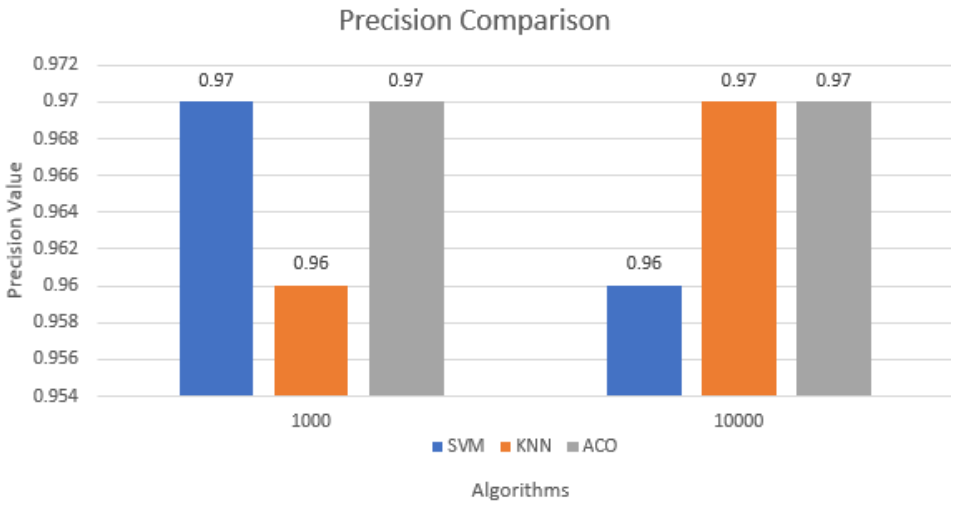

Figure 5: Precision Comparison between the algorithms

to Support vector machine and K-nearest neighbour algorithm. Ant colony optimization algorithm provides the highest accuracy of 98.15% over 10,000 samples of dataset. Whereas, SVM provides the lowest accuracy of 94.68% over 10,000 number of samples. Using SVM, we have observed that on increasing the dataset size, the accuracy is reduced. This is due to increase in the number support vectors.

7 Conclusion and Future Work

From all the observations, we can come to a conclusion that Ant Colony Optimization (ACO) provides the highest accuracy of 98.15%. The data generated synthetically is very much similar to real world network data. Therefore, we can say that in the production system used for finding the illegal access point should use the Ant colony Optimization technique, as it provides the low false positive rate and higher accuracy as compared to other models. In the future work, the different genetic algorithms can be explored. From some studies, we have also found that ensemble learning methods provides the high accuracy using discrete features for binary classification. In future work, we can compare the existing work with Random forest, AdaBoost and many other classifiers.

References

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[2] O. P. Akomolafe and A. I. Adegboyega, "An improved knn classifier for anomaly intrusion detection system using cluster optimization," 2017.

[3] B. AL-Madani, A. Shawahna, and M. Qureshi, "Anomaly detection for industrial control networks using machine learning with the help from the inter-arrival curves," 11 2019.

[4] S. Mathur and A. Badone, "A methodological study and analysis of machine learning algorithms," *International Journal of Advanced Technology and Engineering Exploration*, vol. 6, pp. 45–49, 02 2019.

[5] B. Alotaibi and K. Elleithy, "Rogue access point detection: Taxonomy, challenges, and future directions," *Wireless Personal Communications*, vol. 90, pp. 5021– 5028, 10 2016.

[6] V. Bhusari, "Application of hidden markov model in credit card fraud detection," *International Journal of Distributed and Parallel systems*, vol. 2, 11 2011.

[7] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal, and W. K. Mashwani, "A survey on intrusion detection and prevention in wireless ad-hoc networks," *Journal of Systems Architecture*, vol. 105, p. 101701, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1383762119305089

[8] R. R. Reddy, Y. Ramadevi, and K. V. N. Sunitha, "Effective discriminant function for intrusion detection using svm," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2016, pp. 1148–1153.

[9] Asaju, L. Bolaji, P. B. Shola, N. Franklin, and H. M. Abiola, "Intrusion detection system on a computer network using an ensemble of randomizable filtered classifier , k-nearest neighbor algorithm," 2017.

[10] J. Hounsou, T. Nsabimana, and J. Degila, "Implementation of network intrusion detection system using soft computing algorithms (self organizing feature map and genetic algorithm)," *Journal of Information Security*, vol. 10, pp. 1–24, 01 2019.

[11] B. Jahromy, A. Honarvar, M. Saif, and M. Jahromy, "A new method for detecting network intrusion by using a combination of genetic algorithm and support vector machine classifier," vol. 11, pp. 810–815, 01 2016.