Machine Learning and Deep Learning Techniques for Intrusion Detection in Cyber Security: A Comprehensive Review and Future Directions

Mrs.M.Mahabooba[1], Dr.P.Megaladevi[2], Dr.M Ramesh Kumar[3], Kirthiga R[4], M.S.Vinu[5]

[1]Assistant Professor (SG), Computer Science and Engineering,

Nehru Institute of Engineering and Technology,Coimbatore,

[2]Professor and Dean, Management Studies, Jai Shriram Engineering College, Tirupur

[3]Professor, Information Technology, V.S.B. College of Engineering Technical Campus, coimbatore

[4]Assistant professor in Artificial Intelligence and Data Science, Builders Engineering College, Tirupur

[5]Assistant Professor, CSE, Nehru Institute of Engineering and Technology, Coimbatore

ABSTRACT

With the development of the Internet, cyber-attacks are changing rapidly and the cyber security situation is not optimistic. Machine Learning (ML) and Deep Learning (DL) methods for network analysis of intrusion detection and provides a brief tutorial description of each ML/DL method. Papers representing each method were indexed, read, and summarized based on their temporal or thermal correlations. Because data are so important in ML/DL methods, they describe some of the commonly used network datasets used in ML/DL, discuss the challenges of using ML/DL for cyber security and provide suggestions for research directions.

1. INTRODUCTION

CYBER SECURITY

An interruption detection system is programming that screens a solitary or a system of PCs for noxious exercises that are gone for taking or blue penciling data or debasing system conventions. Most procedure utilized as a part of the present interruption detection systems are not ready to manage the dynamic and complex nature of digital assaults on PC systems. Despite the fact that effective versatile strategies like different systems of machine learning can bring about higher detection rates, bring down false caution rates and sensible calculation and correspondence cost. With the utilization of information mining can bring about incessant example mining, order, grouping and smaller than normal information stream. Cyber Security depicts an engaged writing review of machine learning and information digging techniques for digital investigation in help of interruption detection. In view of the quantity of references or the pertinence of a rising strategy, papers speaking to every technique were distinguished, perused, and compressed. Since information are so essential in machine learning and information mining approaches, some notable digital informational indexes utilized as a part of machine learning and information digging are portrayed for digital security is displayed, and a few proposals on when to utilize a given technique are given.

INTRUSION DETECTION

Intrusion Detection System (IDS) is meant to be a software application which monitors the network or system activities and finds if any malicious operations occur. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks. This main objective of this intrusion detection is to provide a complete study about the definition of intrusion detection, history, life cycle, types of intrusion detection methods, types of attacks, different tools and techniques, research needs, challenges and applications.

MACHINE LEARNING

Machine learning is one of the most exciting recent technologies in Artificial Intelligence. Learning algorithms in many applications that’s they make use of daily. Every time a web search engine like Google or Bing is used to search the internet, one of the reasons that works so well is because a learning algorithm, one implemented by Google or Microsoft, has learned how to rank web pages. Every time Face Book is used and it recognizes friends&#39; photos, that&#39;s also machine learning. Spam filters in email saves the user from having to wade through tons of spam email, that&#39;s also a learning algorithm. Machine learning, a brief review and future prospect of the vast applications of machine learning has been made.

SUPERVISED LEARNING

This learning process is based on the comparison of computed output and expected output, that is learning refers to computing the error and adjusting the error for achieving the expected output. For example a data set of houses of particular size with actual prices is given, then the supervised algorithm is to produce more of these right answers such as for new house what would be the price.

UNSUPERVISED LEARNING

Unsupervised learning is termed as learned by its own by discovering and adopting, based on the input pattern. In this learning the data are divided into different clusters and hence the learning is called a clustering algorithm. One example where clustering is used is in Google News (URL news.google.com). Google News groups new stories on the web and puts them into collective news stories.

REINFORCEMENT LEARNING

Reinforcement learning is based on output with how an agent ought to take actions in an environment so as to maximize some notion of long-term reward. A reward is given for correct output and a penalty for wrong output. Reinforcement learning differs from the supervised learning problem in that correct input/output pairs are never presented, nor sub-optimal actions explicitly corrected.

2. LITERATURE SURVEY

ANEVALUATION FRAMEWORK FOR INTRUSION DETECTION DATASET

AmirhosseinGharib et al., has proposed in these paper the growing number of security threats on the Internet and computer networks demands highly reliable security solutions. Meanwhile, Intrusion Detection (IDSs) and Intrusion Prevention Systems (IPSs) have an important role in the design and development of a robust network infrastructure that can defend computer networks by detecting and blocking a variety of attacks. Reliable benchmark datasets are critical to test and evaluate the performance of a detection system. There exist a number of such datasets, for example, DARPA98, KDD99, ISC2012, and ADFA13 that have been used by the researchers to evaluate the performance of their intrusion detection and prevention approaches. However, not enough research has focused on the evaluation and assessment of the datasets themselves. In this paper we present a comprehensive evaluation of the existing datasets using our proposed criteria, and propose an evaluation framework for IDS and IPS datasets.

CHARACTERIZATION OF ENCRYPTED AND VPN TRAFFIC USING TIME-RELATED FEATURES

Gerard Draper Gil et al., has proposed in these paper Traffic characterization is one of the major challenges in today’s security industry. The continuous evolution and generation of new applications and services, together with the expansion of encrypted communications makes it a difficult task. Virtual Private Networks (VPNs) are an example of encrypted communication service that is becoming popular, as method for bypassing censorship as well as accessing services that are geographically locked. In this paper, we study the effectiveness of flow-based time-related features to detect VPN traffic and to characterize encrypted traffic into different categories, according to the type of traffic e.g., browsing, streaming, etc. We use two different well-known machine learning techniques (C4.5 and KNN) to test the accuracy of our features. Our results show high accuracy and performance, confirming that time-related features are good classifiers for encrypted traffic characterization.

UNSW-NB15: A COMPREHENSIVE DATA SET FOR NETWORK INTRUSION DETECTION SYSTEMS (UNSW-NB15 NETWORK DATA SET)

Moustafa et al., has proposed in these paper one of the major research challenges in this field is the unavailability of a comprehensive network based data set which can reflect modern network traffic scenarios, vast varieties of low footprint intrusions and depth structured information about the network traffic. Evaluating network intrusion detection systems research efforts, KDD98, KDDCUP99 and NSLKDD benchmark data sets were generated a decade ago. However, numerous current studies showed that for the current network threat environment, these data sets do not inclusively reflect network traffic and modern low footprint attacks. Countering the unavailability of network benchmark data set challenges, this paper examines a UNSW-NB15 data set creation. This data set has a hybrid of the real modern normal and the contemporary

NETWORK ATTACKS AND THEIR DETECTION MECHANISMS: A REVIEW

Nikhil S. Mangrulkar et al., has proposed in these paper with the development of large open networks, security threats for the network have increased significantly in the past few years. Different types of attacks possess different types of threats to network and network resources.Many different detection mechanisms have been proposed by various researchers. This paperreviews different type of possible network attacks and detection mechanisms proposed byvarious researchers that are capable of detecting such attacks.

RELATED WORK

There are many puzzles about the relationship among ML,DL, and artificial intelligence(AI). AI is a new technological science that studies and develops theories, methods, techniques ,and applications that simulate, expand and extend human intelligence. It is a branch of computer science that seeks to understand the essence of intelligence and to produce a new type of intelligent machine that responds ina manner similar to human intelligence. Research in this area includes robotics, computer vision, nature language processing and expert systems. AI can simulate the information process of human consciousness, thinking. AI is not human intelligence, but thinking like a human might also exceed human intelligence. ML is a branch of AI and is closely related to (and often overlaps with) computational statistics, which also focuses on prediction making using computers. It has strong ties to mathematical optimization, which delivers methods, theory and application domains to the field. ML is occasionally co fixated with data mining, but the latter subfield focuses more on exploratory data analysis and is known as unsupervised learning. ML can also be unsupervised and be used to learn and establish baseline behavioral paroles for various entitiesand then used to nd meaningful anomalies.

The differences between ML and DL include the following:

Data dependencies. The main difference between deep learning and traditional machine learning is its performance as the amount of data increases. Deep learning algorithms do not perform as well when the data volumes are small, because deep learning algorithms require a large amount of data to understand the data perfectly. Conversely, in this case, when the traditional machine learning algorithm uses the established rules, the performance will be better

Hardware dependencies. The DL algorithm requires many matrix operations. The GPU is largely used to optimize matrix operations efficiently. Therefore, the GPU is the hardware necessary for the DL to work properly. DL relies more on high-performance machines with GPUs than do traditional machine-learning algorithms.

Feature processing. Feature processing is the process of putting domain knowledge into a feature extractor to reduce the complexity of the data and generate patterns that make learning algorithms work better. Feature processing is time consuming and requires specialized knowledge. In ML, most of the characteristics of an application must be determined by an expert and then encoded as a data type. Features can be pixel values, shapes, textures, locations, and orientations. The performance of most ML algorithms depends upon the accuracy of the features extracted. Trying to obtain high level features directly from data is a major difference between DL and traditional machine-learning algorithms Thus; DL reduces the effort of designing a feature extractor for each problem. Problem-solving method. When applying traditional machine-learning algorithms to solve problems, traditional machine learning usually breaks down the problem into

multiple sub problems and solves the sub-problems, ultimately obtaining the final result.In contrast, deep learning advocates direct end-to-end problem solving.

Execution time. In general, it takes a long time to train a DL algorithm because there are many parameters in the DL algorithm; therefore, the training step takes longer. The most advanced DL algorithm, such as ResNet, takes exactly two weeks to complete a training session, whereas ML training takes relatively little time, only seconds to hours. However,the test time is exactly the opposite. Deep learning algorithms require very little time to run during testing.

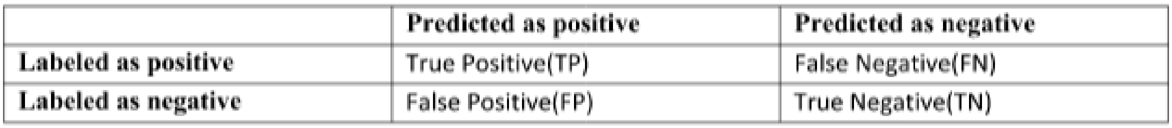
Compared with some ML algorithms, the test time increases as the amount of data increases. However, this point does not apply to all ML algorithms, because some ML algorithms have short test times Interpretability. Crucially, interpretability is an important factor in comparing ML with DL. DL recognition ofhandwritten numbers can approach the standards of people,a quite amazing performance. However, a DL algorithm will not tell why it provides this result. Of course, from a mathematical point of view, a node of a deep neural networkis activated.

Thus, it isdifficult to explain how the result was generated. Conversely,the machine-learning algorithm provides explicit rules forwhy the algorithm chooses so; therefore, it is easy to explain the reasoning behind the decision.

The steps of a DL approach are similar to ML, but as mentioned above, unlike machine-learning methods; its featureextraction is automated rather than manual. Model selection is aconstant trial and error process that requires a suitableML/DL algorithm for different mission types. There are three types of ML/DL approaches: supervised, unsupervised and semi-supervised. In supervised learning, each instance consistsof an input sample and a label. Thesupervised learning algorithm analyzes the training data and uses the results of the analysis to map new instances. Unsupervised learning is a machine-learning task that deduces the description of hidden structures from unlabeled data. Because the sample is unlabeled, the accuracy of the algorithm&#39;s output cannot be evaluated, and only the key features of the data can be summarized and explained. Semi-supervised learning is a means of combining supervised learning with unsupervised learning. Semi-supervised learning uses a large amount of unlabeled data when using labeled data for pattern recognition using semi-supervised learning can reduce label efforts while achieving high accuracy.

Commonly used ML algorithms include for example K-Nearest Neighbor(KNN),MRF, Decision Tree, and Bayes. The DL model includes for example Deep Belief Network(DBM),Convolutional Neural Network (CNN), and Long-Short Term Memory(LSTM).There are many parameters such as the number of layers and nodes to choose, but also to improve the model and integration. After the training is complete, there are alternative models that must be evaluated on different aspects. The evaluation model is a very important part of the machine-learning mission. Different machine learning missions have various evaluation indicators, whereas the same types of machine-learning missions also have different evaluation indicators, each with a different emphasis such as classification, regression, clustering and the like. The confusion matrix is a table that describes the classification results in detail, whether they are correctly or incorrectly classified and different classes are distinguished, for a binary classification a 2 * 2 matrix, and for n classification, an n * n matrix.

TABLE 1. Confusion matrix



	Predicted as positive	**Predicted as negative**
Labeled as positive	True Positive(TP)	False Negative(FN)
Labeled as negative	False Positive(FP)	True Negative(TN)

Predicted as positive Predicted as negative

Labeled as positive True Positive(TP) False Negative(FN)

Labeled as negative False Positive(FP) True Negative(TN)

- True Positive (TP): Positive samples correctly classified by the model;
- False Negative (FN): A positive sample that is misclassified by the model;
- False Positive (FP): A negative samples that is misclassified by the model;
- True Negative (TN): Negative samples correctly classified by the model;

Further, the following metrics can be calculated from the confusion matrix:

- Accuracy: (TP + TN)/ (TP + TN + FP + FN). Ratio of the number of correctly classified samples to the total number of samples for a given test data set. When classes are balanced, this is a good measure; if not, this metric is not very useful.

- Precision: TP/ (TP + FP). It calculates the ratio of all “correctly detected items” to all “actually detected items”.
- Sensitivity or Recall or True Positive Rate (TPR): TP/ (TP + FN). It calculates the ratio of all “correctly detected items” to all “items that should be detected”.
- False Negative Rate (FNR): FN/ (TP + FN). The ratio of the number of misclassified positive samples to the number of positive samples.
- False Positive Rate (FPR): FP/ (FP + TN). The ratio of the number of misclassified negative samples to the total number of negative samples.
- True Negative Rate (TNR): TN/ (TN + FN). The ratio of the number of correctly classified negative samples to the number of negative samples.
- F1-score:2*TP / (2*TP + FN + FP).It calculates the harmonic mean of the precision and the recall.
- ROC: In ROC space, the abscissa for each point is FPR and the ordinate is TPR, which also describes the trade-off of the classifier between TP and FP. ROC&#39;s main analysis tool is a curve drawn in ROC space - the ROC curve.

In the area of Cyber Security, the metrics commonly used in assessment models are precision, recall, and F1-score. The higher and better the precision and recall of model tests are, the better, but in fact these two are in some cases contradictory and can only be emphatically balanced according to the task needs. The F1-score is the harmonic average of precision and recall, considering their results. In general, the higher the F1-score, the better the model will perform.

CONCLUSION

In this paper, we have proposed a new approach to detect the emergence of topics in a social network stream.The basic idea of our approach is to focus on the social aspect of the posts reflected in the mentioning behavior of users instead of the textual contents. We have combined the proposed mention model with the MRF change-point detection algorithm .The signature based detection gives higher detection accuracy and lower false positive rate but it detects only known attack but anomaly detection isable to detect unknown attack but with higher false positive rate.The Intrusion Detection System plays a very significant role in identifying attacks in network. There are various techniques used in IDS like signature based system, anomaly based system. But Signature based system can detect only known attack, unable to detect unknown attack but anomaly based system is able to detect attack which is unknown. Here Anomaly based system with integrated approach using multi-start metaheuristic method is defined.

REFERENCES

1. Sharafaldin, I, Lashkari,A.H and Ghorbani, A.A, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization”, 4th International Conference on Information Systems Security and Privacy (ICISSP), Purtogal, (2018).

2. Gharib, A., Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A., “An Evaluation Framework for Intrusion Detection Dataset”. 2016 IEEE International Conference Information Science and Security (ICISS), pp. 1-6, (2016)

3. Gil, G.D., Lashkari, A.H., Mamun, M. and Ghorbani, A.A., “Characterization of encrypted and VPN traffic using time-related features. In Proceedings of the 2nd International Conference on Information Systems Security and Privacy, pp. 407-414,(2016).

4. Moustafa, N. and Slay, J., “The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 dataset”. Information Security Journal: A Global Perspective, 25(1-3), pp.18-31, (2016).

5. Moustafa, N. and Slay, J., “UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). IEEE Military Communications and Information Systems Conference (MilCIS), pp. 1-6, (2015).

6. Pongle, Pavan, and GurunathChavan. &quot;A survey: Attacks on RPL and 6LoWPAN in IoT.&quot; IEEE International Conference on Pervasive Computing, (2015).

7. Oh, Doohwan, Deokho Kim, and Won Woo R, &quot;A malicious pattern detection engine for embedded security systems in the Internet of Things.&quot; Sensors, pp, 24188-24211, (2014).

8. Mangrulkar, N.S., Patil, A.R.B. and Pande, A.S., “Network Attacks and Their Detection Mechanisms: A Review”. International Journal of Computer Applications, 90(9), (2014).

9. Kasinathan, P., Pastrone, C., Spirito, M. A., &amp;Vinkovits, M. “Denialof-Service detection in 6LoWPAN based Internet of Things.” In IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications, pp. 600-607, (2013).