An Efficient Classifier for U2R, R2L, DoS Attack

Piyush gupta

Abstract.The internet has become an irreplaceable communicating and informative tool in the current world. With the ever-growing importance and massive use of the internet today, there has been interesting from researchers to find the perfect Cyber Attack Detection Systems (CADSs) or rather referred to as Intrusion Detection Systems (IDSs) to protect against the vulnerabilities of network security. CADS presently exist in various variants but can be largely categorized into two broad classifications; signature-based detection and anomaly detection CADSs, based on their approaches to recognize attack packets.The signature-based CADS use the well-known signatures or fingerprints of the attack packets to signal the entry across the gateways of secured networks. Signature-based CADS can only recognize threats that use the known signature, new attacks with unknown signatures can, therefore, strike without notice. Alternatively, anomaly-based CADS are enabled to detect any abnormal traffic within the network and report. There are so many ways of identifying anomalies and different machine learning algorithms are introduced to counter such threats. Most systems, however, fall short of complete attack prevention in the real world due system administration and configuration, system complexity and abuse of authorized access. Several scholars and researchers have achieved a significant milestone in the development of CADS owing to the importance of computer and network security. This paper reviews the current trends of CADS analyzing the efficiency or level of detection accuracy of the machine learning algorithms for cyber-attack detection with an aim to point out to the best. CADS is a developing research area that continues to attract several researchers due to its critical objective.

I. INTRODUCTION

Internet security is one of the most vital requirements in the modern era. With lots of information and data being passed across the internet today, serious businesses, informative and educational networks highly consider investing in network security to ensure the safety of their data from unauthorized access. Today, there
exists a constant threat of various attacks on the data and the data users making the invention of Intrusion Detection Systems very essential. CADS have the capability to detect and avert malicious attacks on the networks, normalize the network functionality during attacks as well as undertake informed security analysis. These important capabilities explain their wide adoption by network administrators. The need to realize safe and secure exchanges on networks has seen increased use CADS, various hardware and software solutions, authentication and encryption just to avoid the ever-present network cyber-attacks.
Cyber-attacks represent a new wave to networks security and can no longer be assumed thus requires careful consideration as a matter of importance.

The current trends in CADS study show intensive concerns to detect and report novel attacks and not just coming up with a Reliable CADS. More emphasis has been placed to ensure no imminent threats are left unreported. Nonetheless, no components of CADS have been found to be wholly impermeable with the guarantee of a cyber-attack remains a massive problem thereby prompting a concurrent quest to find out the most efficient approach for detection. The shortcoming of the CADS creates to identify new patterns and recognize new attacks presents the need for CADS to work along with human experts since they cannot be trusted on their own. It is worth to note that the latest generation of CADS has come a long way but there is a need for further improvement.

II. CYBER ATTACKS.

This is a compound term for any attempts made to override a computer's security system. These attempts impact negatively on the availability, confidentiality and integrity of the network's resources. Cyber-attacks can broadly be classified into four major categories:

2.1 Denial of Service Attacks (DOS)

This is the most dangerous class of cyber-attacks that acts by creating a lot of traffic within the computing or memory resource making it too full thereby unable to handle requests by legitimate users of the system. Examples of this attack include Back, Smurf, TCP SYN flooding, Land, Teardrop and Neptune.

2.2 Remote to Local (User) Attacks (R2L)

This class of attacks sends packets to the network with an intention of prying on their vulnerabilities to gain illegal local access to resources that exist on that network. They include Ftp-Write, Xsnoop, Guest and the Dictionary that target misconfigured or weak system securities. Xlock attack is another that uses social engineering to gain access.

2.3 User to Root Attacks (U2R)

Buffer overflow is the most common of U2R attacks. This class begins by gaining access to a normal user while sniffing around for passwords to gain access as a root user to a computer resource.

2.4 Probing

Probing is a class of attack where the attacker probes a network for vulnerabilities such as open ports that can be used to identify services that run on the resource. They often obtain privileged access to a non-expecting host through an identified vulnerability.

Revised Manuscript Received on April 16, 2020.
Piyush gupta' Research scholor,Department of CSEUniversity institute of technologyAffiliated toRgpv bhopalgpiyush524@gmail.com

III. MACHINE LEARNING APPROACH

Arthur, S. (1959) defines machine learning as a study through which a computer gains knowledge without being programmed. These are categorized into three namely; supervised learning, unsupervised learning, and reinforcement learning.

3.1 Supervised Learning

Also known as classification, here data are labelled during training. Some examples of learning algorithms include; Artificial Neural Network, Lazy learning, Support Vector Machine, Bayesian Statistics, Bayesian Networks, Gaussian Process Regression, K-nearest neighbour, Naïve Bayes classifier among others.

3.2 Unsupervised Learning

Here data instances remain unlabeled prominently done using clustering technique. Common examples include Cluster analysis, Hierarchical clustering, Self-organizing map among others.

3.3 Reinforcement Learning

In this approach, the computer interacts with an environment to meet its goal. An example is a domain expert being asked to label an instance from the unlabeled data set.

4. Single classifiers

A single machine learning algorithm for developing a cyber-attack detection system can be implemented as a single classifier.

Decision Tree

Decision tree rides on its simplicity and easy implementation for its popularity. The algorithm can be expanded into Classification tree with a range of symbolic class label and Regression tree with a range of numerically valued class labels.

Naïve Bayes

Tipped for classification in cases of simpler relations as it only requires a single scan of the training data.

K-nearest neighbor

Described as the simplest and nonparametric for sample classification.(Bishop, 1995). K-nearest neighbour is more of an instance-based learner and not inductive based (Mitchell, 1997).

Artificial Neural Network

In this, the neural networks are arranged in layers made up of interconnected nodes that carry along the function of activation. The layers are interconnected from input to output for the production of the detection result.(Haykin, 1999)

Support Vector Machines

Classifiers built on Support Vector machines systematically discriminates the input space with the remaining space considered to contain anomalies.(Carlos A. Catatnia, 2012).

4.6Fuzzy Logic:

These algorithms go beyond the truth values of true or false and are more relaxed enabling truth to exist somewhere and not necessarily at the absolute false or truth.(Zimmermann, 2010)

5. Hybrid Classifiers:

In a bid to improve the CADS performance, these classifiers are made up of more than one algorithm. They employ either supervised or unsupervised learning approaches as the first level hybrid classifier.(Chih-Fong Tsai, 2009)

6. Ensemble Classifiers:

Multiple weak learners can be combined through bagging, boosting and majority vote strategies for improved performance. Ensemble Classifier is gaining popularity by the day due to some outstanding performances in some areas and researchers are gaining interest in them by the day. However, one shortcoming is that the challenges of individual weak learners are accumulated.(Dewan Md. Farid, 2011)

IV. COMPARATIVE ANALYSIS

The past decade has seen a lot of research intended to improve machine learning algorithms approaches for intrusion detection to satisfy the growing need for intelligent CADS. The approaches realize intrusion detection in different ways. Some of the classifications works available in literature have been discussed as below.

7.1 layered approach

Layered approach borrows its motivation from airport security where checks are done in a sequential fashion to ensure integrity, availability and confidentiality of data over a network. The layered approach reduces the computation time for anomaly detection and improve the system's performance.

7.2 least squares support vector machine:

This is a supervised learning method from a modification of the standard SVM. It is effective as it avoids local minima in SVM problems and is useful in the detection of normal and data attacks.

7.3 Neuro-tree classifier:

This was proposed by Sindhu et al (SS Sivatha Sindhu, 2012,Appl 39) and its features are selected by genetic-based approach for classification. This approach is well known for its low rate of false alarm and added swift convergence.

7.1 Linear programming system-based method for detecting U2R attacks.

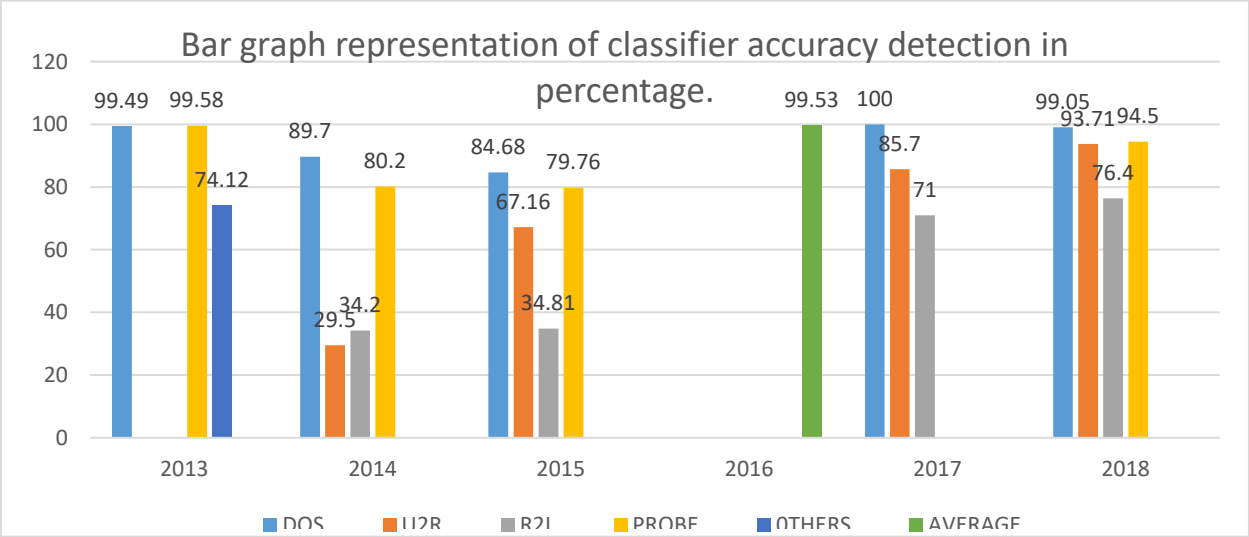
This is a proposed optimal algorithm that is hailed for effective classification of attacks.

Comparison:

The linear method is more efficient in the detection of U2R attacks however for effective security provision there should be the focus on all the types of attack.The layered approach is highly effective in detecting all kinds of attack since every attack is analyzed on separate layers. The Least square support vector machine based classification avoids the local minima and therefore detects all kind of attacks with improved accuracy.Neuro-tree classifier requires optimal features for it to provide an effective classification. When optimal features are provided it has reduced false alarm rate while its algorithms converge fast.

Table 1. Overview of detection accuracy trend of sampled classifiers in related works between 2013-2018.

Researchers	Reference	Classifier	Detection Accuracy
Ganapathy et al 2013	(Ganapathy & Koluthungan, 2013)	IAEMSVM IREMSVM	PROBE - 99.58, DOS - 99.49, OTHERS - 74.12 PROBE - 99.67 DOS - 99.58 OTHERS - 74.22
Kim & Kim 2014	(kim & Kim, 2014)	HFR-MLR	PROBE - 80.2 DOS - 89.70 U2R - 29.5 R2L - 34.20
Hamed, H et al 2015	(Pajour & Dastghaibyfard, 2015)	Two-tier classification model based on NAÏVE BAYES + CF-KNN	PROBE – 79.76 DOS – 84.68 U2R – 67.16 R2L – 34.81
Akhilesh Kumar et al 2016	(Shrivas & Mishra, 2016)	ENSEMBLE MODEL Combining C4.5 and Classification and Regression Tree (CART) approach.	AVERAGE ACCURACY – 99.53
Uma R., Suresh N. 2017	(Salunkhe & Mali, 2017)	Ensemble model using a hybrid approach combining data level feature level approach	DOS – 100 U2R – 85.7 R2L - 71
Divyasree T.H; Sherly K.K 2018	(T.H & K.K, 2018)	Ensemble CVM Using Efficient Feature Selection Approach	PROBE – 94.50 DOS – 99.05 R2L – 76.4 U2R – 93.71



V. CONCLUSION

.This paper presents a review of the literature on the classifiers' efficiency for cyber-attack detection focusing on the past five years. It is clear that the most effective method of intrusion detection is yet to be established. Every single approach to implementing a CADS is effective in their own ways and has specific downfalls as pointed out in the comparison. This makes it extremely difficult to pick on a specific method for implementation over the others. Therefore, it is not realistic to come up with single CADS that would rightly classify all the attacks targeted towards a system. It is wise to preprocess datasets owing to their numerous features and tremendous volume in order to increase their information value for a speedier intrusion detection process. Several approaches presented in this case still require implementation of new methodologies for reduced input feature without compromising on system accuracy. As of the trend, the future should look into coming up with a more efficient technique way that would reduce the input dataset.

REFERENCE

1. Bishop, C. (1995). Neural networks for pattern recognition. oxford, England: Oxford University.
2. Carlos A. Catatnia, F. (2012). An autonomous labeling approach to support vector machines algorithms for network traffic anomaly detection. Expert Systems with Applications.
3. Chih-Fong Tsai, Y.-F. H.-Y.-Y. (2009). Intrusion detection by machine learning. ELSERVIER. Dewan Md. Farid, M. Z. (2011).

Adaptive Intrusion Detection based on Boosting. International Journal of Computer Applications.
4. Ganapathy, S., & Koluthungan, k. (2013). Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP Journal on Wireless Communications and Networking, 14.
5. Haykin, S. (1999). Neural Networks: A comprehensive foundation (2nd edition). New Jersey: Prentice Hall.
6. kim, E., & Kim, S. (2014). A Novel Anomaly Detection System Based on HFR-MLR Method. Mobile, Ubiquitous and Intelligent computing, 274, 279-286.
7. Mitchell, T. (1997). Machine Learning. New York: MacHraw Hill.
8. Pajour, H. H., & Dastghaibyfard, G. (2015). Two-tier network anomaly detection model: a machine learning
9. approach. Journal of Information systems.
10. Salunkhe, U. R., & Mali, S. N. (2017). Security Enrichment in Intrusion Detection System Using Classifier
11. Ensemble. Journal of Electrical and Computer Engineering.
12. Shrivas, A. K., & Mishra, P. K. (2016). Intrusion Detection System for Classification of Attacks with Cross
13. Validation. International Journal of Engineering Science Invention, 21-24.
14. SS Sivatha Sindhu, S. G. (2012,Appl 39). Decision tree based light weight intrusion detection using a wrapper
15. approach. *Expert systems*, 129-141.
16. T.H, D., & K.K, S. (2018). A Network Intrusion Detection System Based On Ensemble CVM Using Efficient
17. Feature Selection Approach. procedia computer science.
18. Zimmermann, H. _. (2010). Fuzzy set theory. Advanced review. John Wiley & Sons, Inc.