Research Paper Computer Science

Classification of Intrusion Detection Into True Positive, False Positive and False Negative by Probabilistic Approach

S. Vaithyasubramanian Research Scholar, Sathyabama University, Chennai, India.

Dr. A.Christy Research Supervisor, Sathyabama University, Chennai, India.

ABSTRACT

As PCs and access to the Internet get to be more pervasive, current society is getting to be progressively reliant on the PC and systems administration innovation for communicating information through email, data storage, online shopping, booking online tickets, reading articles via internet and etc. Identifying unlawful, unauthenticated practices of the host or system is the real question of Intrusion Detection System (IDS). In fact the Intrusion Detection System (IDS) is such a helpful structure to recognize the illegal and unauthorized admittance in a network. One of the capacity of IDS is it could screen different exercises on the system. IDS will send a notice message to the administrators in the event that it recognizes an intrusion and attack. Rapidly, the point of intrusion detection is to categorize harmful attacks by the intruders. The intrusion practice causes immense harm to the systems. System specialists, Application developers search for intrusion detection system (IDS) to ensure the network and systems are safe. In this paper, we presented a mathematical framework to model an intrusion detection system and to classify intrusion in to true positive, false positive and false negative. The results elaborating the classification are presented in the form of graph based on the intrusion and normal behavior.

KEYWORDS Network Security, Intrusion detection, Intrusion Prevention, TP, FN, FP, Alarm, Bayesian Inference.

I. INTRODUCTION

Modern endeavors in the field of network security are empowering regarding frameworks created to guarantee the security of the systems related to information hoard and assurance. With the perpetually expanding requests of velocity and thickness or volume of the information that must be kept up in the IT business and in addition household applications like web has postured genuine difficulties of system security or interruption anticipation or recognition. Storage based intrusion detection system (SIDS) has turned into a profitable instrument in observing for the intrusion. Intrusion detection is a security innovation that endeavors to recognize and detach "intrusions" against computer systems. Providing security to system Intrusion detection plays a key, critical role as an obstruction to attacks, future attacks and also it complements other protection technologies. An intrusion detection system (IDS) assesses all inbound and outbound system action and recognizes suspicious paradigms that may show a system or framework attack from somebody endeavoring to break into or barter a framework. At Present there are a small number of approaches to sort an intrusion detection system (IDS). In misuse detection, the intrusion detection system (IDS) investigates the data it accumulates and contrasts it with extensive databases of attack signature.

Basically, the intrusion detection system (IDS) searches for a particular attack that has as of now been archived. In anomaly detection, the framework overseer characterizes the standard, or ordinary, condition of the network traffic load, breakdown, convention, and average packet size. The anomaly detector screens system portions to contrast their state with the ordinary gauge and search for anomalies. In a network based framework, or NIDS, the individual packets moving through a network are examined. The NIDS can distinguish pernicious packets that are intended to be ignored by a firewall short-sighted sifting tenets. In a host-based framework, the intrusion detection system (IDS) looks at the progress on every individual PC or host. Network based IDS (NIDS) screens activity between hosts while host-construct IDS screen movement in light of the hosts themselves. Host-based IDS as a rule inspects client action and system based IDS typically looks at the yield of a packet sniffer. In indiscriminate mode, the network interface will get all traffic on the local network section as opposed to simply the packets tended to it.

In a Passive system, the IDS recognize a potential security break, logs the data and signs a caution. In a reactive system, the IDS react to the suspicious action by logging off a client or by reinventing the firewall to square system activity from the suspected malignant source. As far as possible the entrance between systems with a specific end goal to forestall interruption and does not flag an attack from inside the system. An intrusion detection system (IDS) assesses a suspected interruption once it has occurred and signals a caution. An intrusion detection system (IDS) additionally looks for attacks that start from inside a system. An IPS is utilized as a part of PC security. It gives arrangements and principles to system activity alongside an intrusion detection system for alarming network or system administrators to suspicious traffic, however permits the overseer to give the activity after being cautioned. Some contrast an IPS with a blend of IDS and an application layer firewall for indemnity.

In this paper we propose a method for intrusion detection using probabilistic approach with the principle of Bayesian inference and it is carried out by using Java programming. The classification of the alert produced by the system is then classified into True positive or false positive or false negative. In this paper a successful attempt is made to detect the intrusion in the network system and to classify them as TP, FN and FP. The remainders of the paper are organized as follows. Section II describes about the terminologies on intrusion detection systems. Section III portraits Bayesian Inference, the methodology used in this paper and also sketch our proposed methodology. Section IV shows the experiments results and its representation in the form of graph and Section V is conclusions.

III. TERMINOLOGIES

The traditional modernism, for instance, firewall is utilized to protect from attacks. The IDS (Intrusion Detection System) are by and large used to promote the system security. The important major characteristic in the focus of firewall and IDS framework is that firewall is a physical simple security framework. Similarly, IDS could gather bundles online from the sys-

tem. In the wake of gathering them, IDS will screen and investigate these parcels. In this way, IDS framework goes about as the "second line of protection". Finally it will furnish and provides the system administrators the results. The identifying results could be either assault or ordinary conduct. A perfect IDS framework has a 100% assault identification rate alongside a 0% false positive rate; however it is difficult to accomplish. The largest parts NIDSs accentuate both viability and proficiency in the intervening time.

Classically satisfactoriness is measured by detection rate and false alert rate, and ability is measured by reacting time for an attack take place. The terminologies concerning to intrusion and Alert classification is as follows: Detection Rate: The detection rate is exemplified as the measure of intrusion event recognized by the system (True Positive) partition by the aggregate number of intrusion cases display in the test set. False Alarm Rate: Characterized as the measure of "ordinary" instance named attacks (False Positive) estranged by the combined number of "typical" instance. Alert/Alarm: A sign recommending that a system has been or is being attacked. True Positive: An authentic attack which triggers an intrusion detection system (IDS) to create an alert. False Positive: An occurrence indication of an intrusion detection system (IDS) to deliver a caution when no attack has occurred. False Negative: A disappointment of an intrusion detection system (IDS) to identify a real assault. True Negative: When no attack has occurred and no alert is raised. Noise: Data or impedance that can trigger a false positive or dark a true positive. Alarm filtering: The methodology of organizing attack cautions delivered from an intrusion detection system (IDS) to recognize false positives from true attacks.

Intrusion	Alarm	Classification
Yes	Yes / 1	TP
Yes	No / 0	FN
No	Yes / 1	FP
No	No / 0	TN

Table: 1 Classification of Alarm and Intrusion

IV. Probabilistic Modeling of Intrusion Detection:

In Statistics, to outline fuzziness about information, the information will be modeled and expressed in terms of probability by a standard advance known as Bayesian Inference. The preliminary step of this Bayesian is to draw a model near to the description of about the information in such a way that there is more than enough justification to exemplify. Subsequently from the ambiguous parameters of the model prior probabilities are derived intended to catch our convictions about the circumstance before seeing the information. Third stage and the final step is by applying Bayes rule in the previously observed some information; to acquire a posterior appropriation on those questions, which makes note of both the prior and the information. For further observation good number of inferences and conclusion about the data can be derived from the computed probability values.

The method has been proposed in a way that it will do analysis on network packets and log files of the system. It will analyze each network packets and session by session log to derive with probability value called as prior probability. And based on this probability alert will be produced such as P (A/IB), P (A/NB). Then from the derived prior probabilities such as P (IB), P (NB), P (A/IB) and P (A/NB) posterior probabilities P (IB/A) and P (NB/A) will be computed which leads to the classification of intrusion and alert produced. If P (NB/A) < P (IB/A), it indicates the effective functioning of the intrusion detection system i.e. the system is said to be Passive system. If P (NB/A) > P (IB/A) point outs the defects of the IDS. The posterior probabilities are computed

as: $P(IB/A) = \frac{P(IB)\,P(A/IB)}{P(IB)\,P(A/IB) + P(NB)\,P(A/NB)}$,

$P(NB/A) = \frac{P(NB)P(A/NB)}{P(IB)P(A/IB) + P(NB)P(A/NB)}$ Where IB: Intrusion Behavior, NB: Normal Behavior, A: Alarm / Alert.

Intrusion Detection Classification:

```
Read i/p Network Traffic (NT)
Read i/p system Log (SL)
Conversion Network Traffic data to Probability Value
Conversion System Log data to Probability Value
NT in → Probability P (NB), P (IB), P (A/NB), P (A/IB)
L in → Probability P (NB), P (IB), P (A/NB), P (A/IB)
NB – Normal Behavior, IB – Intrusion Behavior
Alarm (A) Integer Value 0 or 1,
//Input parameters
P (NB), P (IB), P (A/NB), P (A/IB)
Integer alarm A;
Print Input parameters
//Output parameters
P (A), P (IB/A), P (NB/A)
Print Output parameters
//Formula implementation for P (IB/A)
P (A) = P (IB) * P (A/IB) + P (NB) * P (A/NB);
P (IB/A) = {P (IB) * P (A/IB)} / P (A);
P (NB/A) = {P (NB) * P (A/NB)} / P (A);
Compute P (A); P (IB/A); P (NB/A)
Print P (A); P (IB/A); P (NB/A)
//checking for conditions to check for intrusion
If {{P (IB/A) >= 0.3 && alarm A == 1}
Then print ("Intrusion happened"[TP]) ;}
Else if {{P (IB/A) >= 0.3 && alarm A == 0}
Then print ("Intrusion may happen; But not known"[FN]) ;}
Else if {{P {IB/A) < 0.3 && alarm == 1}
Then print ("Intrusion not happened"[FP]) ;}
```

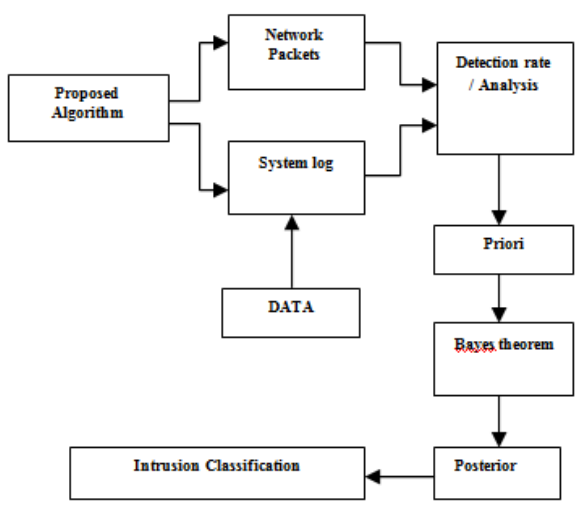

Fig: 1 proposed method Architecture

V. Results and Graph:

From the computed prior probabilities, posterior probabilities and alarm generated 50 random samples are analyzed and they are plotted in the form of graphs. The inferences are tabulates in classifying the intrusion behavior. The graphs and inference tables are plotted on the nature of intrusion behavior given Alarm, Normal Behavior given Alarm, Intrusion behavior and Normal behavior.

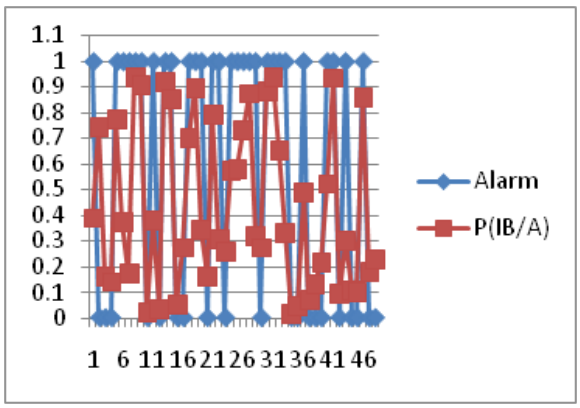

Fig: 2 Intrusion Behaviour and Alert - P(IB/A)

Sample No.	Intrusion	Alarm	Classification
2	Yes	0	FN
7	No	1	FP

Table: 2 Intrusion Classification Based on P(IB/A)

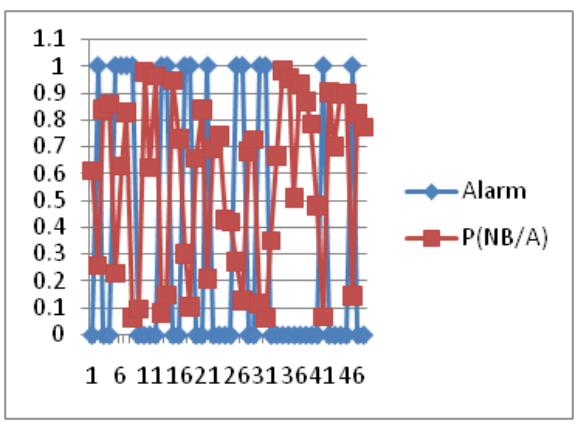

Fig: 3 Normal Behaviour and Alert - P(NB/A)

Sample No.	Intrusion	Alarm	Classification
7	No	1	FP
8	No	1	FP
9	Yes	0	FN

Table: 3Intrusion Classification Based on P(NB/A)

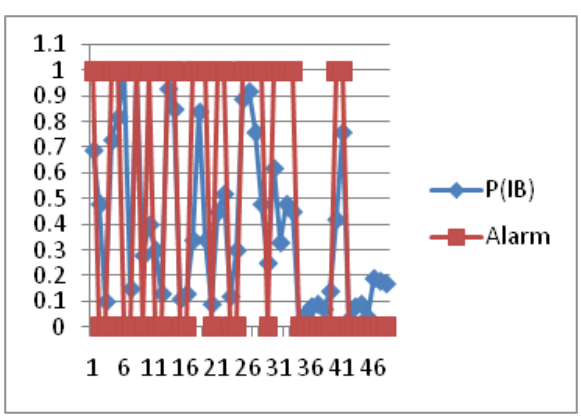

Fig: 4 Intrusion Behaviour and Alert - P(IB)

Sample No.	Intrusion	Alarm	Classification
2	Yes	0	FN
7	No	1	FP

Table: 4 Intrusion Classification Based on P(IB)

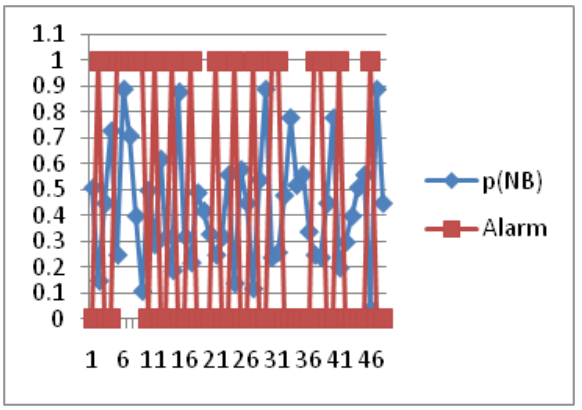

Fig: 5 Intrusion Behaviour and Alert - P(NB)

Sample No.	Intrusion	Alarm	Classification
7	No	1	FP
8	No	1	FP
9	Yes	0	FN

Table: 5 Intrusion Classification Based on P(NB)

Conclusion

In the existing and the upcoming research area of network security and information security Intrusion detection prolongs to be a dynamic and hot topic. Numerous analysts and professionals are effectively tending to these issues. Constant development, advancement in this field emerges still system administrator's faces difficulties and problems in solving this issue. Moreover a lot of false alerts relics an uncertain problem in detecting unidentified prototype of the attacks, which reflects in the efficiency of the system. Good number of inferences can be drawn from the above results, which include the classification of intrusion also. For improved security mechanisms in computer network security this method of applying Bayesian inference in Network Intrusion Detection can pave a new way. Even though in recent times, quite a few consequences comprise exposed there is a likely decision on this issue. End users will be benefited once the problems get solved. The assessing and benchmarking of IDSs is also an important problem. The practical functioning, execution and performance of IDS will improve if the synthesis of IDS and its end result attack alert are reformed optimally. We anticipate that Intrusion detection will turn into a common sense and compelling answer for ensuring data frameworks.

REFERENCES

[1]. Sandip Sonawane, Shailendra Pardeshi and Ganesh Prasad "A survey on intrusion detection techniques" World Journal of Science and Technology 2012, 2(3):127-133, ISSN: 2231 – 2587. | [2]. Victor-Valeriu Patriciu, Liviu Rusu, Iustin Priescu "Data Mining Approaches for Intrusion Detection in Email System Internet-Based" 144-147. | [3]. Wenke Lee Salvatore J. Stolfo "Data Mining Approaches for Intrusion Detection" Proceeding SSYM'98 Proceedings of the 7th conference on USENIX Security Symposium - Volume 7. | [4]. Aikaterini Mitrokotsa, Nikos Komninos, and Christos Douligeris "Protection of an Intrusion Detection Engine with | Watermarking in Ad Hoc Networks" International Journal of Network Security, Vol.10, No.2, PP.93–106, Mar. 2010. | [5]. Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks" International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, 44 – 52, April 2009. | [6]. Mahendra Singh Sisodia, Sanjay Kumar Sharma, Pankaj Pandey , Susheel Kumar Tiwari "Anomaly Based Network Intrusion Detection by using Data Mining "International Journal of Advanced Research in Computer Science and Electronics Engineering, Volume 1, Issue 1, 33 – 38, March 2012. | [7]. Sang-Jun Han and Sung-Bae Cho "Evolutionary Neural Networks for Anomaly Detection Based on the Behavior of a Program" IEEE Transactions on Systems, Man, and Cybernetics—Part b: Cybernetics, VOL. 36, No. 3, 559 – 570, June 2006. | [8]. Rupali Datti1, Bhupendra verma "Feature Reduction for Intrusion Detection Using Linear Discriminant Analysis" International Journal on Computer Science and Engineering Vol. 02, No. 04, 1072-1078, 2010. | [9]. Rajdeep Borgohain "Fuzzy Genetic paradigms in Intrusion Detection Systems" Int. J. Advanced Networking and Applications, Volume: 03, Issue: 06 Pages: 1409-1415, 2012. | [10]. Jianxiong Luo "Mining Fuzzy Association Rules and Fuzzy Frequency Episodes for Intrusion Detection" International Journal of Intelligent Systems, Volume 15, No. I, August 2000. | [11]. Ambareen Siraj, Rayford B. Vaughn, Susan M. Bridges "Decision Making for Network Health Assessment in An Intelligent Intrusion Detection System Architecture" Journal of Information Technology and Decision Making. | [12]. Kanok Prothives and Surat Srinoy "Integrating ART and Rough Set Approach for Computer Security" Proceedings of the International MultiConference of Engineers and Computer Scientists, Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong. | [13]. Rung-Ching Chen 1, Kai-Fan Cheng 2 and Chia-Fen Hsieh "Using Rough Set and Support VectorMachine for Network Intrusion Detection" International Journal of Network Security & Its Applications (IJNSA),Vol 1, No 1, April 2009 | [14]. Radford M. Neal, "Philosophy of Bayesian Inference", http://www.cs.toronto.edu/~radford/res-bayes-ex.html, January 1998. | [15]. Jun Zhu, Ning Chen "Bayesian Inference with Posterior Regularization and Applications to Infinite Latent SVMs" Journal of Machine Learning Research 15 (2014) 1799-1847. | [16]. https://bayesian.org/Bayes-Explained. | [17]. www.danielowen.com. | [18]. http://mathworld.wolfram.com/BayesianAnalysis.html. | [19]. S. Vaithyasubramanian, A. Christy "A Study on Markov Chain Password using Bayesian Inference" Artificial Intelligent Systems and Machine Learning, ISSN 0974 – 9543, Vol 6, No 3 (2014). | [20]. S. Vaithyasubramanian, A. Christy "Bayesian inference based intrusion detection" – National Conference on Mathematical and computational Modeling – NCMCM12, 27 – 29 June 2012, Sathyabama University, Chennai, ISBN 978 – 81 – 923853-0-3, Page No. 153 – 157. |