A Survey: Intelligent Intrusion Detection System in Computer Security

Parveen Sadotra
CEH, Research Scholar,
Department of computer science
Career point University,
Kota, Rajasthan

Chandrakant Sharma, PhD
Assist. Professor,
Department of computer science
Career point University,
Kota, Rajasthan

ABSTRACT
Now a day's fast broadcast of computer networks has changed the perspective of network security. An easy availability of circumstances cause computer network as vulnerable beside numerous threats from hackers. Threats to networks are various and possibly devastating. Up to the instant, researchers have established Intrusion Detection Systems (IDS) proficient of identifying attacks in numerous presented environments. A boundlessness of approaches for misuse detection as well as anomaly detection has been functional. Numerous of the tools projected are balancing to each other, since for different kind of surroundings some methods achieve better than others. This paper presents an evaluation of intrusion detection systems that is then used to study and classify them. The taxonomy involves of the detection principle, and another of positive working features of the intrusion detection system.

Keywords
IDS, security, Network, WSN, SVM

1. INTRODUCTION
The Intrusion detection systems (IDSs) are an important component of a broad defense-in-depth construction for computer network security. IDS are an actual security knowledge, which can detect, prevent and probably respond to the attack [1]. It displays target sources of actions, assembles and reviews review data looking for indication of invasive performances. Once it detects apprehensive or malicious attempts, an alarm is raised up giving the network manager the chance to react prompt. The key objective of IDS is to sense all intrusions in an effectual manner. IDSs can be confidential from dissimilar facts of view. Figure 1 displays different classifications of IDSs. From the view of detection technique, IDSs can be separated into two groups: anomaly and misuse (signature) based detection.

Anomaly detection attempts to control whether deviation from the recognized usual practice patterns can be identified as intrusions. On the other hand, misuse detection uses designs of well-known attacks or weak spots of the system to recognize intrusions [2]. As revealed in Figure 1, contingent on the info source, an IDS might be either host or network-based. A host-based IDS (HIDS) examines measures such as procedure identifiers and system calls, mostly connected to OS evidence. On the other hand, a network-based IDS (NIDS) investigates network connected actions: traffic volume, IP addresses, service ports, protocol usage, etc. [3]. Though IDS keys have been used for around twenty years, a significant problem is silent not completely addressed: Unfortunately, these systems run on enormous number of alerts which maximum of them are false alerts or low position. For instance, a single IDS device can produce tens of thousands of signals in a day [4, 5]. Great volume of signals is uncontrollable and overpowering to the human forecaster. Reviewing thousands of signals per day is impractical, particularly if 99% of them are false alerts [6]. False alerts, also known as false positives occur when a legitimate activity has been incorrectly secret as malicious by the IDS. The huge inequality between the definite and false alarms produced has definitely destabilized the presentation of IDS [7].

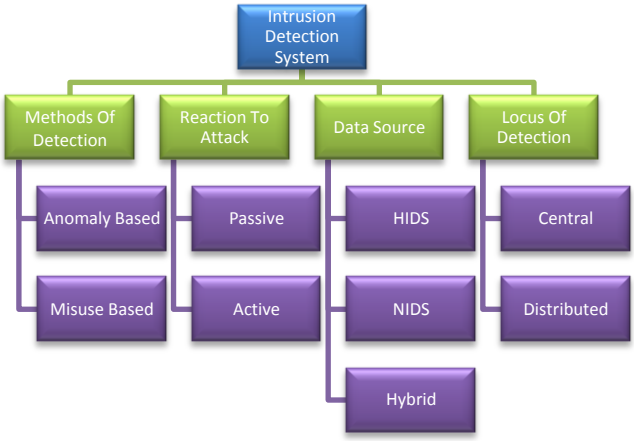

Fig. 1 Characteristics of intrusion detection system

Although those anomaly-based IDSs generate extra false positives rather than misuse-based IDSs, false positives are obvious in all kinds of IDS. Since of these details, through the previous few years' false positives reduction methods have been widely investigated [4] and researches on IDSs have absorbed on how to switch these warnings.

2. LITRATURE SURVEY
A current review [10, 11] declares that intrusions inside the governments are rising exponentially. To circumvent such intrusions the planned outline has authorized with movable representatives to perceive intrusions in a rapid time below the assumed environment. In instruction to sense user anomalies, the normal user action profiles are produced and a parallel score range (upper and lower bound) is allocated to each user's normal design set. When in action, the system computes the similarity score of the current activity's patterns, and if this score is not in the similarity score range, the activity is considered as an anomaly.

Yogitha et. al. [8] Offered intrusion detection system with Support Vector Machine (SVM). Confirmation is done by directing investigates on NSL-KDD Cup'99 data set which is reformer form of KDD Cup'99 data set. By using this NSL-KDD Cup'99 data set they have condensed wide time compulsory to shape SVM classic by accomplishment proper pre-processing on data set. In this organization is done by using SVM. By responsibility proper kernel collection attack detection rate is amplified and false positive rate (FPT) is reduced. In this proposed work author has used Gaussian Circular Basis.

Wenke Lee et. al. [9] has first tried to mine the system review data to study reliable use full tapping of database and user performance. They have also used the usual of applicable system features accessible in the designs to calculate inductively learned classifiers that can identify irregularities and identified intrusions. In instruction to make the classifier an actual model they should have a necessary inspection data for training and a set of analytical system features. To controller the review data and feature selection they have future the suggestion rule and numerous incidents from the audit data, which is used in organization model. They have combined field knowledge into these basic procedures using the alignment and position attributes.

Eleazar, Matthew et. al. [10] offered an adaptive model generation, a technique for automatically building detection classical for data mining based intrusion detection system. The data composed by intrusion detection sensor models are used to realize this. The detection models are efficient by the systems mechanically as more data is composed. Adaptive model generation may meaningfully decrease the cost of organizing an IDS system because it eliminates the essential for physically creating training set.

S.A. Joshi, et. al.[11] In this paper the author deliberate about the data mining procedures and Intrusion detection system to detect the unidentified attacks from the dataset. There different classes of attacks but the authors of this paper deliberate the few types of attacks. They associates the four kinds of attacks are:

a) Probing attack

b) Denial of service

c) User to root

d) Remote to local

Formerly the author registered out the numerous data mining methods and intrusion detection methods which are used for the perceiving the attacks similar signature based detection, irregularity based detection, and network- based intrusion detection system, host-based detection system. Associating these types of attacks and conclusion the high detection rates. Pattern taking algorithm has high detection rate. Lastly, the invention out the percentage for detection rate and false alarm rate.

Sushil Kumar Chaturvedi, et. al. [12] the foremost effort of these associates two types of algorithms C4.5 and Support Vector Machine (SVM). First the assumed dataset is pre-processing and then the data can be partition into training and testing. The 3rd phase the dataset is functional in C4.5 and SVM algorithm. The author of this paper associates these two algorithms and discovery out the detection rate assessment and false alarm rate assessment. By using these two data mining methods they validate the C4.5 algorithm is better than the support vector machine.

Omprakash Chandrakar, et. al.[13] this work defines around basic notions of system intrusion detection system, mechanisms and kinds of attacks. The IDS covers the 3types of mechanisms specifically data source, analysis engine, response manager. This paper provides the impression of genetic algorithm. The genetic algorithm casually selected the input (chromosome) and computes the fitness value for each produced initial chromosome. The iteration has achieved some precise processes namely sorting, selection, crossover, mutation and lastly computesthe fitness value for chromosome.

A.R. Jakhale, et. al [14] In this work the author describes an anomaly detection system and its two phases specifically training and testing. The descending window and clustering is used to nursing the network traffic by mining the recurrent patterns using algorithms. The algorithms are so actual and used in real time observing. The common multi-pattern capturing algorithm has high detection rate. Finally, novelty the proportion for detection rate and false alarm rate.

R. Venkatesan, et al.[15] This author defines an anomaly detection system and its two stages specifically training and testing. The sliding window and clustering is used to observing the network traffic by mining the recurrent patterns using algorithms. The algorithms are so active and used in real time monitoring. The normal multi-pattern capturing algorithm has high detection rate. To end with find the percentage for detection rate and false alarm rate.

Abhilasha A Sayar, et.al.,[16] In this paper the author deliberate about the classification of Intrusion detection system, beneficial and detrimental and its types. In this the IDS uses theartificial intelligence, fuzzy logic and neural network. The methods are used to detect the intrusions in the images.For example, in soldierly the original information's are different into images and then send to another site. Byusing the artificial intelligence with IDS the user can simply classify the unknown attacks. This paper is valuable for beginners to study the basic ideas of Intrusion detection system and also notice all kind of images.

Table 1: Comparitive Study

Author(s)	Year	Paper name	Technique	Result
Ayei E. Ibor	2015	A Hybrid Justification Technique for Malicious Network Traffic based on Active Response	HYBRITQ-4(J48, Boyer Moore, KNN)	High detection rate and low false positive rate.
AnnkitaPatel,Risha Tiwari	2014	Bagging Ensemble Technique for intrusion Detection System	Bagging & Boosting: SVM &Decision Tree	Combination of two algorithms is better than other ensemble technique.

Yogita B.Bhavsar& Kalyani C. Waghmare	2013	Intrusion Detection System Using Data Mining Technique Support Vector Machine	Data Mining , SVM	Detection rate is increased & False positive rate is decreased.
Rowayda A.Sadek, M. Sami Soliman& Hagar S. Elsayed	2013	Effective Anomaly Intrusion Detection System based on Neural Network with Indicator Variable and Rough set Reduction	NNIV-RS	High detection rate and low false positive rate
Ahemd A Elngar,Dowalt, Fayed	2013	A Real Time Anomaly Intrusion Detection System with High Accuracy	PSO-Discritize-HNB	High detection accuracy and speed up the time
HeshamAltwaijry, Saeed Algarny	2012	Bayesian based Intrusion Detection System	Bayesian Probability	Achieved better detection rate with low threshold value
Renuka DeviThanasekaran	2011	A Robust & Efficient Real Time Network Intrusion Detection System Using Artificial Neural Network in Data Mining	ANN: Binary Classification and Multi boosting	Time taken to detect the attack is decreased
Naveen N. C., R.Srinivasn, S. Natarajn	2010	A Unified Approach for Real Time Intrusion Detection using Intelligent Data Mining Techniques	SLFN	Faster attack detection compared to others
Tao Peng, WanliZuo	2006	Data mining Intrusion Detection System in real time	Data Mining: FP Tree & FP Growth	Resource consuming for feature extraction and efficiency are satisfied.
Wanke Lee,Salvotore J Stolfa	2000	Adaptive Intrusion Detection: A Data Mining Approach	Association Rule &Frequent Episode	Made classifier as an effective model

3. ISSUES AND CHALLENGES IN IDS

These days intrusion detection system is quiet in beginning and essential lot of investigation work to be done to kind the intrusion detection even more positive. There are a vast number of matters and challenges in current intrusion detection system which wants the instantaneous and robust research attention. In this paper, we have acknowledged some significant issues and challenges which need to be addressed by research societies. The issues and challenges are as:

- Deficiency or incomplete Data set
- Detection Algorithms
- Integration of multiple formats of data
- Platform dependencies
- Poor Design
- Testing/ Evaluation of IDS

We will discuss all the issues and challenges in detail as under:

A.Data Set

The data set can be definite as a group of all the data or info through the survey which wants to be examined. Since, in intrusion detection system, the data sets show important role in accuracy of results. Thus it developed very much important to have datasets which are almost near to real time system. Now a day, the researchers are using data set DARPA 98, 99, New Mexico University protected organization etc. but being out-of-date, we are not intelligent to alleviate those attacks which are very much new.

B.Detection policy

This is the key part though novelty whether the packet/ information originate is attack or the valuable information which the user requirements to instrument the procedure or jobs. The detection algorithm should be capable enough that it must match all the case in small time and also should bout the positions resourcefully. The discovery policy may be either anomaly or misuse based. In anomaly based detection, the behaviour is recognized and if behaviour is recognized as contrary of normal, it is professed as attack and in additional situation, the pattern is coordinated using some pattern corresponding algorithm for recognized attacks and if pattern matches fully with some doubtful data, it is professed as attack. But there are also disadvantages that there are no rules for new attacks to be coordinated, hence new attacks are not detected or if it kinds some changes in data so that it cannot match the pattern, the attack is noticed. Hence we are in need of good and fast algorithm which will detect the pattern systematically and fast to match the most of the attacks.

C.Integration of Multiple formats

As we are well conscious of the detail that the external frames or data might be in dissimilar arrangements. So there is need that different arrangements shall be combined on a single intrusion detection system. i.e. on the fly it should check for the arrangements and check the torrent for intrusions.

D.Platform Dependence

In present technical world, we have different number of intrusion detection system obtainable some are free source while other are profitable. While applying these intrusion detection systems all of them have system conditions to device the intrusion detection software. Consequently wants some platform for application. As we do have different platforms, we need intrusion detection software which may be

platform autonomous so that we can device the same intrusion detection software on all the platforms.

E. Poor design

The project of all the intrusion detection systems are dense i.e. if a user want to change some portion of the intrusion detection system, we have to stay the intrusion detection system, then complete the changes as anticipated and re-deploy it again. Hence the project of the intrusion detection system must be like as stated below [13]

It must have two parts, one core part which contains of detection algorithm and second part will be the part related with pattern matching. This part should be rationalized on the fly. i.e it should not mark the detection process of the scheme but only informs the other portions without moving core part of the system. Thus each informs should be additional on the fly without ending the intrusion detection system.

F. Testing and evaluation of IDS

As deliberated in the paper, data is increasing extremely and IDS has now developed a normal for getting large network. Corporations are capitalizing enormous quantity in IDS technologies, but there are no such technical approaches to test the efficiency of these IDS. Even though particular measurable quantifiable approaches have been strategy to examination the efficiency, but they do not assess the effectiveness on similar scale. These approaches deliberate reporting or likelihood of false alarm or probability of detection or confrontation to attacks absorbed at IDS or capability of management bandwidth and traffic or capability to classify attacks etc. Hence are not sufficient to figure out efficiency of IDS. Also there should be mutual scale for assessing or testing the efficiency of IDS. The different issues are as [14] [15]:

- Assembling script and victim software
- Different necessities for testing different kinds of IDS
- Challenging with different parameters

4. IMPORTANCE

Subsequently security is of supreme significance in a trade IT infrastructure; there are a lot of profitable contributions from numerous merchants in the intrusion detection and defense space. While most foodstuffs carry a high price tag, there are abstemiously priced products, as well as open source solutions for those absorbed.

Visibility: -An ID delivers a strong assessment of what's going on inside your network. It is an appreciated source of information about distrustful or malicious network traffic. There are few applied replacements to an ID that permits to path network traffic in depth.

Defense: -An ID complements a layer of resistance to security profile, if a useful backstop to some of other security measures.

Response capabilities: - Although they probably will be of limited use, you may want to enable some of the response features of the IDS. For instance, they can be organized to dismiss a user assembly that interrupts policy. Clearly, It necessity reflect the risks of attractive this step, meanwhile you may unintentionally dismiss a legal user assembly. Though, in convinced cases it can be a significant tool to stop damage to the network.

Tracking of virus propagation: -Once virus first successes your network, IDS can tell you which machineries it cooperated, as well as how it is spreading finished the network to contaminate other machines. This can be a great assistance in decelerating or discontinuing a virus's development and making sure remove it.

Evidence: - correctly arranged IDS can produce data that can procedure the basis for a civil or criminal case alongside somebody who wastes your network.

5. DISCUSSION

In beyond numerous works in literature survey accessible by numerous Authors, we examine about various or many present research idea in terms of Support Vector Machine (SVM), NSL-KDD, IDS system, HYBRITQ-4(J48, Boyer Moore, KNN) which are given us to developing technique about intrusion detection system on the base of energy security theme that deliver reliable communiqué and conscious from the intrusion. In WSNs setting each nodes are exploit the information distribution in each assembly and will upsurge the presentation of the network like packet distribution greatness relation, throughput, network life time and minimize the end-to-end delay.

6. CONCLUSION

Intrusion detection techniques have better intensely over time, particularly in the previous few years. Originally developed to systematize monotonous and problematic log parsing activity, IDSs have advanced into cultured, real time applications with the capability to have a comprehensive look at traffic and to sniff out malicious activity. They can handle high-speed networks and multifaceted traffic, and deliver comprehensive vision– before unavailable – into active intimidations in contradiction of critical online information resources. IDS knowledge is emerging quickly and its near-term future is very likely. It is progressively attractive a crucial and essential constituent of any complete enterprise security program, since it accompaniments traditional security instruments. This work runs an impression of the current state of the art of together computer attacks and intrusion detection methods. The impression is based on obtainable classifications demonstrated with the most descriptive examples.

7. REFERENCES

[1] R. Base, P. Mell, "Special publication on intrusion detection systems", NIST Infidel, Inc., National Institute of Standards and Technology, Scotts Valley, CA, 2001.

[2] J. Anderson, "An introduction to neural networks", Cambridge: MIT Press, 1995.

[3] P.G. Teodoro, J.D. Verdejo, G.M. Fernandez, E. Vazquez, "Anomaly-based network intrusion detection: techniques, systems and challenges", Computers Security, 2009.

[4] J. Viinikka, H. Debar, L. Mé, A. Lehikoinen, M. Tarvainen, "Processing intrusion detection alert aggregates with time series modeling", Information Fusion Journal, vol. 10(4), 2009.

[5] R. Vaarandi, "Real-time classification of IDS alerts with data mining techniques", in Proc. of MILCOM Conference, 2009.

[6] K. Julisch, "Clustering intrusion detection alarms to support root cause analysis", ACM Trans. Inf. Syst. Secur. 6, 2003

[7] G.C. Tjhai, S.M. Furnell, M. Papadaki, N.L. Clarke, "A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm", Computers & Security 29, 2010.

[8] Yogita B. Bhavasar, Kalyani C. Waghmare "Intrusion Detection System Using Data Mining Technique: Support Vector Machine" 2013 International Journal of Emerging Technology and Advance Engineering volume 3, Issue 3, March 2013.

[9] WenkeLee ,Salvatore J. Stolfo "Adaptive Intrusion Detection: a Data Mining Approach" 2000

[10] HuyAnh Nguyen, Deokjai Choi "Application of Data Mining to Network Intrusion Detection: Classifier Selection Model"

[11] S.A.Joshi, VarshaS.Pimprale, "Network Intrusion Detection System (NIDS) based on Data Mining", International Journal of Engineering Science and Innovative Technology, Vol. 2, No. 1, January 2013, ISSN. 2319 5967.

[12] Sushil Kumar Chaturvedi, Prof. VineetRichariya. Prof. NirupamaTiwari, "Anomaly Detection in Network using Data mining Techniques", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 5, May 2012, ISSN. 2250-2459.

[13] OmprakashChandrakar, Rekha Singh, Dr. LalBihariBarik, "Application of Genetic Algorithm in IntrusionDetection System", International Institute for Science, Technology and Education, Vol. 4, No. 1, 2014, ISSN. 2224-5774.

[14] A.R. Jakhale, G.A. Patil, "Anomaly Detection System by Mining Frequent Pattern using Data Mining Algorithm from Network Flow", International Journal of Engineering Research and Technology, Vol. 3, No.1, January 2014, ISSN. 2278-0181.

[15] R. Venkatesan, Dr. R. Ganesan, Dr. A. Arul Lawrence Selvakumar., "A Survey on Intrusion Detection using Data Mining Techniques", International Journal of Computers andDistributed Systems, Vol. 2, No. 1, December 2012, ISSN. 2278-5183.

[16] Abhilasha A Sayar, Sunil. N. Pawar, Vrushali Mane., "A Review of Intrusion Detection System in Computer Network", International Journal of Computer Science and Mobile Computing, Vol. 3, No. 2, February 2014, pp. 700 - 703.