IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Concentric Study on Intrusion Detection System Types Tools & Techniques

S. K. Tiwari1*, D. S. Pandey2, V. Namdeo3

[1]Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India
[2] Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India
[3] Computer Science/ Information Technology, RKDF-Institute of Science & Technology, RGPV, Bhopal, India

Available online at: www.ijcseonline.org

Accepted: 18/July/2018, Published: 31/Jul/2018

Abstract— It has become clear that increasing the diversity of types of network networks is becoming a major challenge. This leads to the need to expand the data and exchange more and more information. Intrusion Detection Systems (IDS) are designed to try to eliminate the unauthorized use of this method to detect abuse and misuse of computer systems. In response to the growing use and development of IDS, this would be the most important aspect. In this article, we identify a number of general technical optimizations of the IDS. This article provides methodological details, including intrusion strategies. This article also contains general information about IDS intruders and our work on motivation. This article mainly deals with different methods of optimization and classification. Here, different approaches are mentioned regarding intrusion detection systems.

Keywords: Classifiers, Decryption, Encryption Intrusion Detection System, Optimization techniques, Mobile Agent etc**.**

I. INTRODUCTION

Today Computer System has evolved into a distributed computing machine, nothing is static now, not even the security threats and attacks. The security issues are of high concern today in the world of open system environment. The problem faced widely by the computer system and network is the network intrusion and virus infection. Computer security is an approach to prevent and detect unauthorized use of the device. Preventive measures help prevent unauthorized users from accessing any part of the computer system (also known as "intruders"). Detection helps us determine if someone is trying to enter our system, if it succeeds and what can be done [1]. Computers are used for everything from banking and investing to shopping and communicating with others via e-mail or programs [2]. They probably do not want to see outsiders attacking e-mail computers or attacking other systems, sending fake e-mails or computers, or checking personal information on your computer (for example, financial statements). Intruders (also called attackers, cookies) do not accept our identity [3]. You often want to take control of your computer so that it can perform attacks on other computer systems.

There are various reasons that make burglary detection a necessary part of the entire immune system. First, many traditional systems and applications have been developed without security aspects. In other cases, systems and applications have been designed to work in a different environment and vulnerable to implementation. Intrusion detection complements these protections to improve system security. Even if the preventive security mechanisms can successfully protect information systems, it is still desirable to know what violations have occurred or occur so that we understand the security threats and risks and are therefore better prepared for future attacks.

The attack can be launched in the term of fast attack or slow attack. Fast attack can be defined as an attack that involves a large amount of packet or connection within a few second [7]. Meanwhile, slow attack can be defined as an attack that takes a few minutes to complete [9]. Both of the attack has a great impact on the network environment due to the security breach decade. Axis in Fig: -1, Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack in slow or fast attack. are behavior-based (anomaly) and knowledge-based (misuse) [11], [12]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [13], [14]. The misuse or signature based IDS is a system that contains against a stream or audit data looking for evidence of modeled attack [15]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous data has been revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and character could not be captured using this technique [16, 19].

I.I INTRUSION DETECTION SYSTEM:

DESCRIPTION

Since there is a huge number of categories available to study intrusion detection system because Intrusion is defined as "a set of actions which perform to minimize the confidentiality, integrity or availability of resources.An intrusion detection system is a software program which helps to identify the malicious program which enter our system or in network. It helps to secure our system by responding to the malicious program. Basically It is divided into two types. They are host based intrusion detection system and network based intrusion detection system. The active system will respond to the malicious program. But the passive system will detect only whether any malicious packets entered the system or not [15].Intrusion detection system came into picture around 1980 with the publication of John Anderson's Computer Security Threat Monitoring and Surveillance, which was one of the earliest papers in the field. "An Intrusion Detection Model", published in 1987, provided a methodological framework that inspired many researchers and laid the groundwork for commercial products [20]. An Intrusion Detection System collects all the information from the Host or the networks which include both anomaly and misuse intrusions. Intrusion detection functions include:

- Monitoring and analyzing user activities.
- Analyzing system configurations.
- Assessing system and file integrity.

I.II IDS ARCHITECTURE

Figure 1 represents basic architecture of an intrusion detection system as below:

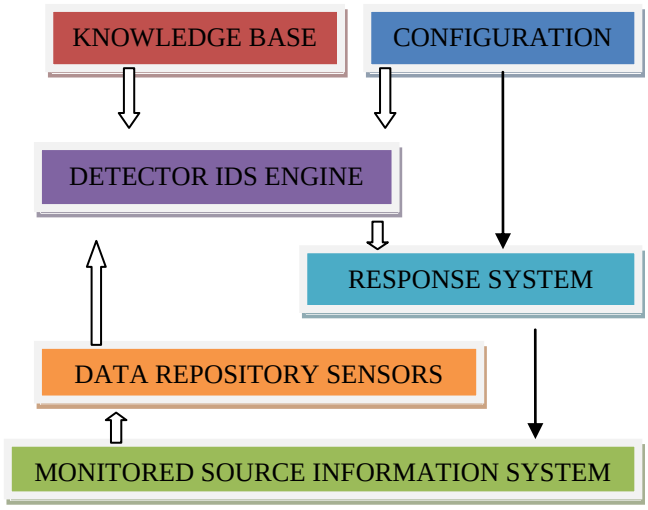

Figure 1: Fundamental IDS Architecture

I.III IDS CATEGORIES

There exist multiple categories of intrusion detection systems according to their functionality and behavior. In general IDS can be categorized in two ways: one is Host based Intrusion Detection System (HIDS) and another one is Network Intrusion Detection System (NIDS).there are some another ways to differentiate IDSs. Hence by the solution schemes and various studies [8, 14, 17 & 18] it is being observed that its many types may exist as shown in Table 1: IDS Types.

Table: 1 IDS Types

S. No.	IDS TYPE	DESCRIPTION
1.	Anomaly Based IDS	Functions with learnt baseline
2.	Signature Based IDS	Functions with known system vulnerabilities
3.	Mobile Agent Based IDS	For various kind of functions different agents used
4.	Network Intrusion Detection Systems (NIDS)	It functions on real time detection concept
5.	Host Intrusion Detection Systems (HIDS)	It works on individual workstation with rich database
6.	Active Intrusion Detection Systems	It can automatically block suspected attacks without any intervention required by an operator
7.	Passive IDS	It only monitor and analyze

I.IV IDS ANALYSIS PARAMETERS

It is very important to become aware with various terminologies of Intrusion Detection System for its better analysis as given here in Table 2 obtained from various researches [17-18]:

Table:2 IDS Parameters

S.No.	PARAMETERS	DESCRIPTION
1.	False Alarms	Events that are not supposed to be occurring in implementation
2.	False Negative	It occurs when attack traffic does not trigger an alert on the IDS device
3.	False Positive	An alert has been triggered, but it was for traffic that does not constitute an actual attack
4.	True Alarms	It is response of IDS
5.	True Negative	It is non-offending or benign traffic did not trigger an alarm
6.	True Positive	A true positive means that the IDS device recognized and responded to

		an attack
7.	Vulnerability	It compromises the security or functionality of a particular system in your network

II. RELATED WORK

To improve the performance of system and the networks by Intrusion detection system, a lot of research work is going on. The research work is focused on in the field of Mobile Agent based Intrusion Detection Systems (MA-IDSs) focusing upon its architecture, technique, strength and weakness is discussed in this paper. In [8] IDS with the integration of Mobile Agents is presented which looks after the anomalies and responds by taking suitable measures with the help of agents. Here in Table 3 various IDS approaches are mentioned.

Table: 3 IDS Approaches

S. No.	APPROACH NAME	DESCRIPTION
1.	IDS on SNORT	Overcome latency ,network load, adapt dynamic environment
2.	Central Coordinator	It imposes light load on entire network
3.	Mobile Agent	Monitoring and functioning handled through different agents
4.	Multilevel Anomalies Detection	Plug-in used to implement such architecture to handle IDS functions
5.	Peer to Peer	In peer to peer IDS, suspicious activities are checked by sending the detection request to other hosts of the system

II.II IDENTIFIESD IDS OBSTACLES & REVIEWS:

There are following basic issues; in the IDS functioning identified:

- Burdensome Maintenance: The configuration and maintenance of intrusion detection systems often requires special knowledge and substantial effort.
- Flexibility: Intrusion detection systems have typically been written for a specific environment and have proved difficult to use in other environments that may have similar policies and concerns. There is a consolidated information in Table 4 given below which contains different agent based IDS approaches and their strengths.
- Lack of efficiencies: This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks.

Table 4: Agent Based IDS Review

S. No.	ARCHITECTURE	TECHNIQUE	STRENGTH
1.	Adhoc based using DSDV	Authentication mechanism(RSA 1024, AES 128) Clustering of mobile agent	Low routing, less overhead
2.	Adhoc based using MA	Bayesian classification	High rate of anomaly, Reduced false alarm
3.	Distributed based using Anomaly detection	Event correlation engine, Agent synergy	Reduced false alarm rate, ID is greater than SNORT
4.	Hybrid and Distributed based using Synchronous & distributed correlation	SynFlooding	Least result of false positive rate, false negative rate, semantic detection
5.	Distributed and Immune based	Dynamic clonal selection algorithm and collaborative signal mechanism	Reduced false positive rate, Increased detection rate
6.	Distributed and SNORT based	Message exchange between server and SNORT	SNORT performance is good
7.	Distributed and Peer To Peer IDS	Retrieval agent generation, retrieval agent dispatch	Efficient migration strategies, MADIDF is better than MASHD
8.	Distributed and central coordinated	Agent based	Less load on entire network, detection more complex

II.III OPTIMIZATION TECHNIQUES

Intrusion detection (ID) is a very important tool which not only detects the intrusion of unauthorized and suspicious activities that can compromise the security pillars (Authentication, availability, Confidentiality and Integrity) IDS use several techniques, which involve the IDS stopping the attack itself, changing the security environment (e.g., reconfiguring a firewall), or changing the attack's content.

The types of IDS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed.
Refer various Optimization techniques are listed below in Table 5:

Table 5: Optimization Techniques

S. No.	OPTIMIZATION TECHNIQUE	DESCRIPTION
1	Network Behavior [21]	examines, network traffic to identify threats that generate unusual traffic flows.
2	Wireless [21]	Technique monitors wireless network traffic and analyzes.
3	Host-based [23]	It uses an agent-console model to agents run on individual hosts but report to a single central control.

II.IV CLASSIFICATION TECHNIQUES

The following criteria will be adopted in the classification of the IPS/IDS:

- Reliability: The generated alerts must be justified and no intrusion to escape.
- Reactivity: An IDS/IPS must be capable to detect and to prevent the new types of attacks as quickly as possible. Thus, it must constantly self-update. Capacities of automatic update are so indispensable.
- Facility of implementation and adaptability: An IDS/IPS must be easy to function and especially to adapt to the context in which it must operate. It is useless to have an IDS/IPS giving out some alerts in less than 10 seconds if the resources necessary to a reaction are not available to act in the same constraints of time.

- ✓ Performance: the setting up of an IDS/IPS must not affect the performance of the supervised systems. Besides, it is necessary to have the certainty that the IDS/IPS has the capacity to treat all the information in its disposition because in the reverse case it becomes trivial to conceal the attacks while increasing the quantity of information.
- ✓ The sources of the data to analyze, network, system or application
- ✓ The behavior of the product after intrusion passive or active
- ✓ The frequency of use, periodic or continuous
- ✓ The operating system in which operate the tools, Linux, Windows, etc.
- ✓ The source of the tools, open or private [24].

Various Classifiers are listed below In Table 6:

Table 6: Classifiers Methods

S. No.	CLASSIFICATION TECHNIQUES	METHOD
1	Soft Computing Based	Neural Network
		Genetic Algorithm
		Fuzzy
2	Tree Based	J48
		ID3
		CART
3	Others	Binary

III. PREVIOUS WORK

Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic In this paper, we focus on different types of attacks on IDS this paper gives a description of different attack on different protocol such as TCP ,UDP,ARP and ICMP [25]

This paper presents WebSTAT, an intrusion detection system that analyzes web requests looking for evidence of malicious behavior. The system is novel in several ways. First of all, it provides a sophisticated language to describe multistep attacks in terms of states and transitions. In addition, the modular nature of the system supports the integrated analysis of network traffic sent to the server host, operating system-level audit data produced by the server host, and the access logs produced by the web server. By correlating different streams of events, it is possible to achieve more effective detection of web-based attacks. [26]
[28]In this paper capturing of network traffic, performance and reports analysis generated by snort and corresponding alert ratio of signatures for the particular attack are to be evaluated. This intrusion detection system is one of the security defense tools for computer networks. In recent years this research has lacked in direction and focus today SNORT stands out as the most widely deployed IDS, We survey the

existing techniques, types and architectures of Intrusion Detection Systems in the literature. Performance analysis of real time Intrusion Detection and prevention system and traffic analysis by Snort from the network are to carried out.

[29] In this system we addressed the dual problem of Accuracy and Efficiency for building robust and efficient intrusion detection systems. This method is much suitable for detecting R2L and U2R attacks.

[30] Here a methodology of applying classification technique for IDS using data mining, in use genetic algorithm into network intrusion detection techniques. A brief overview of Intrusion Detection System (IDS), genetic algorithm, and related detection techniques are discussed.Snort is mostly used signature based IDS because of it is Lightweight and open source software. Basic analysis and security engine (BASE) is also used to see the alerts generated by Snort. In this paper the signature-based Network intrusion detection using Snort and WinPcap implemented.

III.I IDS TOOLS

SNORT: Snort is network intrusion detection and prevention system capable of performing real-time traffic analysis and packet logging on IP networks. Initially called a "lightweight" intrusion detection technology, Snort has evolved into a mature, feature-rich IPS technology that has become the de facto standard in intrusion detection and prevention. With over 4 million downloads and nearly 400,000 registered users, it is the most widely deployed intrusion prevention technology in the world. Snort can perform protocol analysis and content searching/matching [21].

WEKA:

WEKA is a data mining system developed by the University of Waikato in New Zealand that implements data mining algorithms. WEKA is a state-of-the-art facility for developing machine learning (ML) techniques and their application to real-world data mining problems. It is a collection of machine learning algorithms for data mining tasks. The algorithms are applied directly to a dataset. WEKA implements algorithms for data preprocessing, classification, regression, clustering, association rules; it also includes a visualization tools. Here a list of different IDS software tools tabulated below in Table 7:

Table 7: IDS Software & Tools

S. No.	IDS TOOLS	IDS TYPE	OS COMPATIBILITY
1.	AIDE	HIDS	LINUX,UNIX,MAC-OS
2.	Bro	NIDS	LINUX,UNIX,WINDOWS,MAC-OS
3.	Fail2Ban	HIDS	LINUX,UNIX,MAC-OS
4.	Open Wips-NG	NIDS	LINUX
5.	OSSEC	HIDS	LINUX/UNIX,WINDOWS,MAC-OS
6.	Snort	NIDS	LINUX/UNIX,WINDOW

III.II RISK ANALYSIS

Risks in packets: There are some possible risks are enlisted in the Table 8: Risk Table. These are responsible for adverse service behavior.

Table 8: Risk Review

S. No.	INTRUSION & PROTOCOL	DESCRIPTION (RISKS FOR SERVICES)
1.	Teardrop-TCP	Sends overlapping IP fragments.
2.	Smurf -ICMP	The recipients of the directed broadcast ping request respond to the request and flood the target's network.
3.	Open/Close – TCP/UDP	The open/close attack opens and closes connections at a high rate to any port serviced by an external service through intend.
4.	ICMP Redirect -ICMP	ICMP redirects can cause data overload to the system being targeted.
5.	ICMP Unreachable - ICMP	. This causes the TCP session to retry and as more "ICMP unreachable" messages are sent, a DoS condition occurs.
6.	Land –TCP SYN	Source and destination IP addresses are the same causing the response to loop.
7.	Ping of Death-ICMP	ICMP packets greater than 65536 bytes can shut down a system.

IV. CONCLUSION

In this paper mobile agent based Intrusion Detection System critically reviewed. The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system. It is complete study about types of IDS, life cycle, various domains, types of attacks. In the lifecycle OF IDS the phases developed and the stages are illustrated. Still, there are more challenges to overcome. Further on the basis of different techniques goal is to achieve implementation of efficient an effective IDS.

References

[1] A.M. Riyad, M.S. Irfan Ahmed and R.L. Raheemaa Khan "Multi agent based intrusion detection architecture for the IDS adaptation over time", Second International Conference on Electrical, Computer and Communication Technologies (ICECCT),IEEE,2017

[2] Sara Chadli,Mohamed Emharraf and Mohammed Saber "The design of an IDS architecture for MANET based on multi-agent" International Colloquium on Information Science and Technology (CiSt),IEEE,2014

[3] Okan Can "Mobile agent based intrusion detection system", 22nd Signal Processing and Communications Applications Conference (SIU), 2014

[4] Wang Yu, Cheng, Xiaohui and Wang Sheng ,"Anomaly Network Detection Model Based on Mobile Agent", IEEE,Third International Conference on Measuring Technology and Mechatronics Automation, 2011
[5] Jaydip Sen "An Agent-Based Intrusion Detection System for Local Area Networks" published in International Journal of Communication Networks and Information Security (IJCNIS) Vol. 2, No. 2, August 2010 PP 128-140
[6] Mr. Suryawanshi G.R, Prof. Vanjale S.B "Mobile Agent for Distributed Intrusion detection System in Distributed System" Publication in" International Journal of Artificial Intelligence and Computational Research (IJAICR.) ", Jan-June 2010 . ISSN-0975-3974. PP 1-8.
[7] Nicholas J. Puketza, Kui Zhang, Mandy Chung, Biswanath Mukherjee*, Ronald A. Olsson, "A Methodology for Testing Intrusion Detection Systems"
[8] Ionita, I.; Ionita, L. "An agent-based approach for building an intrusion detection system" Published in Networking in Education and Research, 2013 RoEduNet International Conference 12th Edition 26-28 Sept. 2013
[9] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.
[10] Jitendra S Rathore, Praneet Saurabh, Bhupendra Verma "AgentOuro: A Novelty Based Intrusion Detection and Prevention System" Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on 3-5 Nov. 2012
[11] Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002
[12] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.
[13] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J.,,Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference, 2005
[14] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007
[15] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.
[16] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.
[17] Xiao-Yuan Yang , Xuan-Wu Zhou , Ping Wei and Li-Xian Wei"Hybrid NIDS based on biological immunology", Proceedings of 2004 International Conference on Machine Learning and Cybernetics,2004
[18] Qiang Xue , Lin-Lin Guo and Ji-Zhou Sun"The design of a distributed network intrusion detection system IA-NIDS", Proceedings of the 2003 International Conference on Machine Learning and Cybernetics,2003
[19] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.
[20] Anderson, J.P., 1980. Computer Security and Threat Monitoring Surveillance. Technical report at Co. Fort Washington Pennsylvania.
[21] David Geer, Behavior-Based Network Security Goes Mainstream, IEEE,14-17, march 2006
[22] Tiwari Nitin, S. R. Singh and P. G. Singh, Intrusion Detection and Prevention System (IDPS) Technology- Network Behavior Analysis System (NBAS), International Science Congress Association , 51-56, July (2012).
[23] Karen Scarfone, Peter Mell, Guide to Intrusion detection and prevention systems (IDPS), NIST, 1 to 127, 2007.
[24] B. Santos Kumar et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (1) , 2013, 77 – 82, "Intrusion Detection System- Types and Prevention".
[25] Volume 2, Issue 8, August 2012, " An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols".
[26] Giovanni Vigna William Robertson Vishal Kher Richard A. Kemmerer, "A Stateful Intrusion Detection System for World-Wide Web Servers".
[27] C. Krügel, T. Toth, Applying Mobile Agent Technology to Intrusion Detection, ICSE Workshop on Software Engineering and Mobility, 2001
[28] Mukesh Sharma,Akhil Kaushik, Amit Sangwan Performance Analysis of Real Time Intrusion Detection and Prevention System using Snort.,IJERT, July – 2012
[29] Vaishali T.Deshmukh, Shubhangi Vaikole, Layered Crf A Model To Build More Accurate Intrusion Detection System, IJERT, 2012
[30] Bin Zeng , Lu Yao and ZhiChen Chen"A network intrusion detection system with the snooping agents",International Conference on Computer Application and System Modeling, 2010

Authors Profile

Mr. S. K. Sharma pursed Bachelor of Engineering in Information Technology from Rajeev Gandhi Technical University Bhopal (MP), and pursuing Master of Technology in Information Technology from Rajeev Gandhi Technical University Bhopal (MP).

Mr. D. S. Pandey pursed Master of Technology in Information Technology from Rajeev Gandhi Technical University Bhopal (MP), and working as an Assistant professor in Department of Information technology of RKDF-Institute of Science & Technology College Bhopal MP. His main focus is in the field of Data Mining and computer security. He has guided and published more than 20 research papers in various national and international journals.

Dr. V. Namdeo pursed Ph.D. in Computer Science and currently she is working as Head of Department of Computer Science & Engineering and information Technology Department in RKDF-Institute of Science & Technology College Bhopal MP. Her main focus is in the field of Computer Networking, Data Mining, Machine learning and computer security. She has guided and published more than 50 research papers in various national and international journals. She holds experience of teaching over 15 years in her field

