Digital Innovations
& Contemporary Research in SCIENCE,
ENGINEERING & TECHNOLOGY

Vol. 6. No. 4, Dec, 2018

Article Citation Format
Adedibu, O & Adeshipo, M.E. (2018): A Review of Anomaly Detection
Techniques for Intrusion Detection
Journal of Digital Innovations & Contemp Res. In Sc., Eng &
Tech. Vol. 6, No. 4. Pp 1-10

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 27th Oct. 2018
Review Type: Blind
Final Acceptance:: 28th Nov, 2018
DOI Prefix: 10.22624

A Review of Anomaly Detection Techniques for Intrusion Detection

Adedibu, O & Adeshipo, M.E.
Department of Electrical/Electronic Engineering
The Polytechnic, Ibadan
Ibadan, Nigeria
E-mail: ibuacademy@yahoo.co

ABSTRACT

There are a number of common attacks on networked computers which, for their detection, require information from multiple sources, increased network connectivity of computer systems gives greater access to outsiders and makes it easier for intruders to avoid identification, by being connected to a network, computer systems are exposed to different threats and are made more vulnerable to different attacks. This paper discusses anormaly detection techniques utilized for developing intrusion detection systems and provides a general background in terms of literature thus serving as a reference material for further studies into the concepts discussed.

Keywords: Anomaly, detection, intrusion, systems, computers, security and safety

1. INTRODUCTION

A secure computer or network should provide the following services; data confidentiality, data and communication integrity, and assurance against denial of service (http://www.deic.uab.es/material/26118-capitol1.pdf(2015). Data Confidentiality refers to limitinginformation access and disclosure toauthorized users -- "the right people" --and preventing access by or disclosure to unauthorized ones -- "the wrong people." Also critical to confidentiality -- and data integrity and availability as well – are protections against malicious software (malware), spyware, spam and phishing attacks.

Data integrity refers to maintaining and assuring the accuracy and consistency of data over its entire life-cycle, It also includes "origin" or "sourceintegrity" that is, that the data actually came from the person or entity you think it did, rather than an imposter.On a more restrictive view, however, integrity of an information system includes only reservation without corruption of whatever was transmitted or entered into the system, right or wrong (James B. et. al (2011). Data availability refers, unsurprisingly, to the availability of information resources. An information system that is not available when you need it is at least as bad as none at all. An intrusion is an event, or a set of events, that attempts to compromise a computer system's confidentiality, integrity, availability, or that attempts to bypass its securitymechanisms Karen Scarfone et al (2012). Intrusions can be caused by system insiders or by external attackers.

System insiders, or users authorized to use the system, can cause intrusions by attempting to gain privileges to which they are not entitled or by misusing the privileges that have been given to them. External attackers, or users who have not been authorized to use the system, can cause intrusions by gaining access to the system from outside, such as the internet (Karen Scarfone et al 2012). Any unauthorized access or infiltration is called Intrusion (Karen Scarfone et. Al. 2012). For an enterprise to protect itself from abuse of its information, it must monitorthe events occurring in its computer system or network and analyze them forsigns of intrusion. To do this, the enterprise must install an Intrusion DetectionSystem (IDS) Curry et al, (2004).

An intrusion detection system (IDS) is an automated system that aims to detect intrusions in a computer system. The main goal of an IDS is to detect any unauthorized use, abuse, or misuse of computer systems by both system insiders and external attackersAnita K. et al. Its purpose can be compared to that ofa car alarm, which alerts its owner when the car has been broken into. Once an intrusion has been detected, the IDS typically issue an intrusion-response action, which may range from reporting the intrusion to the system administrator, to taking some action against the intruder.

The proliferation of heterogeneous computer networks has serious implication for the intrusion detection problem. Foremost among these implications is the increased opportunity for illegitimate access that is provided by the network's connectivity. This problem is exacerbated when internetwork access is allowed, as well as when unmonitored hosts are present. The use of distributed rather than centralized computing resources also implies reduced control over those resources. Moreover, multiple independent computers generate more audit data than a single computer performing the same amount of user work, and this audit data is dispersed among many systems.

2. REASONS FOR INTRUSION DETECTION SYSTEMS.

By using an IDS, an attack on the computer system can be detected and measures can be taken to stop it before any damage is done to the computer system.

There are several reasons why IDSs are necessary (Marek Piotr Zielinski 2004):

- *To serve as a means to deter those who would violate security policy.* This assumesthat an increased perceived risk of discovery and prosecution of attackers' canprevent certain security problems.
- *To detect attacks and other security violations that other security measures cannot prevent.* An IDS can be used to detect attacks that exploit vulnerabilities in thesecurity mechanisms of a computer system. In addition, an IDS can serve animportant function in protecting the system because it can report intrusions tosystem administrators, who can contain and recover any resulting damage.
- *To detect preambles of attacks.* The first stage of an attack usually involvesexamining a system or network for any vulnerability, searching for an optimalpoint of entry. This stage is often experienced as network probes and other tests forexisting vulnerabilities. By using an IDS, the probes can be detected and action may be taken to block the attacker's access to the target system.
- *To document the existing system threat.* An understanding of the frequency and characteristics of attacks allows understanding of what security measures are appropriate to protect the system.
- *To act as a means of quality control for security design and administration.* An IDS that runs over a period of time can show patterns of system usage and detected problems. These can show the design and management flaws in the system's security. Deficiencies can be corrected before they cause a security problem.

- *To provide information about actual intrusions.* An IDS can collect relevant anddetailed information about the attack, which supports incident handling and recovery efforts. Such information can also be used to identify problem areas in the security configuration or policy of the system.

In addition, IDSs are primarily focused on identifying possible incidents. For example, an IDS could detect when an attacker has successfully compromised a system by exploiting a vulnerability in the system (KarenScarfone, &Mell, 2012). The IDS could then report the incident to security administrators, who could quickly initiate incident response actions to minimize the damage caused by the incident. The IDS could also log information that could be used by the incident handlers. Many IDSs can also be configured to recognize violations of security policies. For example, some IDSs can be configured with firewall rule set-like settings, allowing them to identify network traffic that violates the organization's security or acceptable use policies. Also, some IDSs can monitor file transfers and identify ones that might be suspicious, such as copying a large database onto a user's laptop.

IDSs can also identify reconnaissance activity, which may indicate that an attack is imminent. For example, some attack tools and forms of malware, particularly worms, perform reconnaissance activities such as host and port scans to identify targets for subsequent attacks. An IDS might be able to block reconnaissance and notify security administrators, who can take actions if needed to alter other security controls to prevent related incidents. Because reconnaissance activity is so frequent on the Internet, reconnaissance detection is often performed primarily on protected internal networks(KarenScarfone, &Mell, 2012).

2.1 Common Detection Methodologies

IDS technologies use many methodologies to detect incidents. The following are the primary classes of detection methodologies: signature-based, anomaly-based, and stateful protocol analysis, respectively (KarenScarfone, &Mell, 2012).

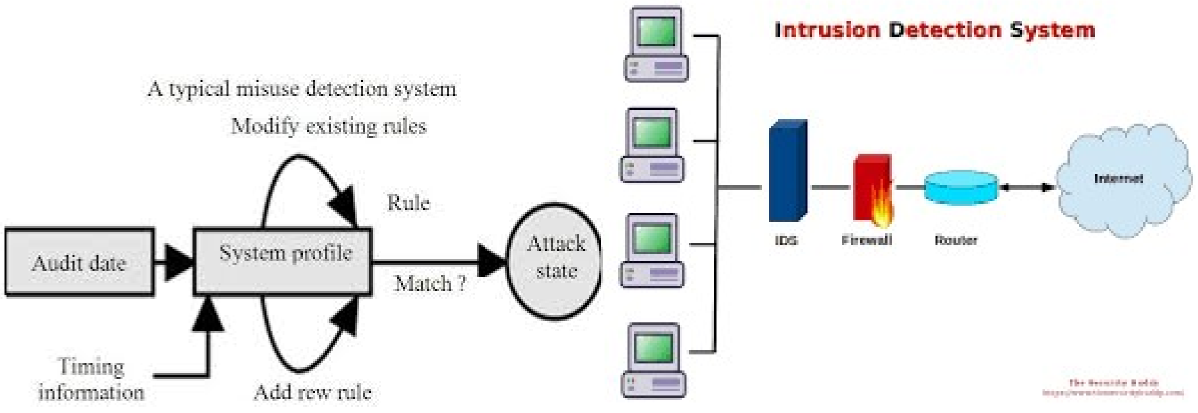

Fig. 1: Anomaly Detection/Intrusion Detection Systems

Most IDSs use multiple detection methodologies, either separately or integrated, to provide more broad and accurate detection. The primary classes of detection methodologies are as follows:

i. **Signature-based**, which compares known threat signatures to observed events to identify incidents. This is very effective at detecting known threats but largely ineffective at detecting unknown threats and many variants on known threats. Signature-based detection cannot track and understand the state of complex communications, so it cannot detect most attacks that comprise multiple events.

ii. **Anomaly-based detection**, which compares definitions of what activity, is considered normal against observed events to identify significant deviations. This method uses profiles that are developed by monitoring the characteristics of typical activity over a period of time. The IDS then compares the characteristics of current activity to thresholds related to the profile. Anomaly-based detection methods can be very effective at detecting previously unknown threats. Common problems with anomaly-based detection are inadvertently including malicious activity within a profile, establishing profiles that are not sufficiently complex to reflect real-world computing activity, and generating many false positives.

iii. **Stateful Protocol Analysis**, which compares predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. It is capable of understanding and tracking the state of protocols that have a notion of state, which allows it to detect many attacks that other methods cannot. Problems with stateful protocol analysis include that it is often very difficult or impossible to develop completely accurate models of protocols, it is very resource-intensive, and it cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior.

2.2 Types of IDS Technologies

There are many types of IDS technologies. For the purposes of this research, they are divided into the following four groups based on the type of events that they monitor and the ways in which they are deployed:

i. **Network-Based**, which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks.

ii. **Wireless**, which monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity involving the protocols themselves. It cannot identify suspicious activity in the application or higher-layer network protocols (e.g., TCP, UDP) that the wireless network traffic is transferring. It is most commonly deployed within range of an organization's wireless network to monitor it, but can also be deployed to locations where unauthorized wireless networking could be occurring.

iii. **Network Behavior Analysis (NBA)**, which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS) attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks).

iv. **Host-Based,** which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

2.3 Typical Components of an IDS

The typical components in an IDS solution are as follows:

- **Sensor or Agent:**Sensors and agents monitor and analyze activity. The term *sensor* is typically used for IDSs that monitor networks, including network-based, wireless, and network behavior analysis technologies. The term *agent* is typically used for host-based IDS technologies.
- **Management Server:**A *management server* is a centralized device that receives information from the sensors or agents and manages them. Some management servers perform analysis on the event information that the sensors or agents provide and can identify events that the individual sensors or agents cannot. Matching event information from multiple sensors or agents, such as finding events triggered by the same IP address, is known as *correlation*. Management servers are available as both appliance and software-only products. Some small IDS deployments do not use any management servers, but most IDS deployments do. In larger IDS deployments, there are often multiple management servers, and in some cases there are two tiers of management servers.
- **Database Server:**A *database server* is a repository for event information recorded by sensors, agents, and/or management servers. Many IDSs provide support for database servers.
- **Console:**A *console* is a program that provides an interface for the IDS's users and administrators. Console software is typically installed onto standard desktop or laptop computers. Some consoles are used for IDS administration only, such as configuring sensors or agents and applying software updates, while other consoles are used strictly for monitoring and analysis. Some IDS consoles provide both administration and monitoring capabilities.

3. EXISTING WORKS IN INTRUSION DETECTION:

The study of security in computer networks is a rapidly growing area of interest because of the proliferation of networks (LANs, WANs etc.), greater deployment of shared computer databases (packages) and the increasing reliance of companies, institutions and individuals on such data. Though there are many levels of access protection to computing and network resources, yet the intruders are finding ways to enter into many sites and systems, and causing major damages. Sothe task of providing and maintaining proper security in a network system becomes a challenging issue. There exist different methods for intrusion detection and the early models includeIntrusion-Detection Expert System(IDES) (later versions (NIDES) and Multics Intrusion Detection and Alerting System(MIDAS)), W & S, AudES, Network Anomaly Detection and Intrusion Reporter (NADIR), Distributed Intrusion Detection System (DIDS), etc (Sanjay Sharma and R. K. Gupta 2015). These approaches monitor audit trails generated by systems and user applications and perform various statistical analyses in order to derive regularities in behavior pattern. These works based on the hypothesis that an intruder's behavior will be noticeably different from that of a legitimate user, and security violations can be detected by monitoring these audit trails.

Most of these methods, however, used to monitor a single host Chandrashekhar A. M and K. Raghuveer (2013),though NADIR and DIDS can collect and aggregate audit data from a number of hosts to detect intrusions. However, in all cases, there is no real analysis of patterns of network activities and they only perform centralized analysis.Recent works include Memon V. I. and Chandel G. S., (2014) and Wankhade K., Patka S. and Thool R., (2013), which used hierarchical graphs to detect attacks on networkedsystems. Other approaches used autonomous agent architectures (Dhakar M. and A. Tiwari, 2012) for distributed intrusiondetection.

3.1 Network-Based IDS

A network-based IDS monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity. This section provides a detailed discussion of network-based IDS technologies. First, it contains a brief overview of TCP/IP, which is background material for understanding the Chapter 3. Next, it covers the major components of network-based IDSs and explains the architectures typically used for deploying the components. It also examines the security capabilities of the technologies in depth, including the methodologies they use to identify suspicious activity.

3.2. Networking Overview

TCP/IP is widely used throughout the world to provide network communications. TCP/IP communications are composed of four layers that work together. When a user wants to transfer data across networks, the data is passed from the highest layer through intermediate layers to the lowest layer, with each layer adding more information. The lowest layer sends the accumulated data through the physical network; the data is then passed up through the layers to its destination.

Essentially, the data produced by a layer is encapsulated in a larger container by the layer below it. The four TCP/IP layers, from highest to lowest, are shown in Table 1.

Table 1: TCP/IP Layers

Application Layer. This layer sends and receives data for particular applications, such as Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP).
Transport Layer. This layer provides connection-oriented or connectionless services for transporting application layer services between networks. The transport layer can optionally ensure the reliability of communications. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are commonly used transport layer protocols.
Internet Protocol (IP) Layer (also known as Network Layer). This layer routes packets across networks. IPv4 is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are IPv6, Internet Control Message Protocol (ICMP), and Internet Group Management Protocol (IGMP).
Hardware Layer (also known as Data Link Layer). This layer handles communications on the physical network components. The best known data link layer protocol is Ethernet.

The four TCP/IP layers work together to transfer data between hosts. Network-based IDSs typically perform most of their analysis at the application layer. They also analyze activity at the transport and network layers both to identify attacks at those layers and to facilitate the analysis of the application layer activity (e.g., a TCP port number may indicate which application is being used). Some network-based IDSs also perform limited analysis at the hardware layer Karen *Scarfone*. Peter *Mell*.(2012).

Network-based IDSs provide a wide variety of security capabilities. Some products can collect information on hosts such as which OSs they use and which application versions they use that communicate over networks. Network-based IDSs can also perform extensive logging of data related to detected events; most can also perform packet captures. Network-based IDSs usually offer extensive and broad detection capabilities. Most products use a combination of signature-based detection, anomaly-based detection, and stateful protocol analysis to perform in-depth analysis of common protocols.

Network-based IDSs have some significant limitations. They cannot detect attacks within encrypted network traffic; accordingly, either they should be deployed where they can monitor traffic before encryption or after decryption, or host-based IDSs should be used on endpoints to monitor unencrypted activity. Network-based IDSs are often unable to perform full analysis under high loads; organizations using inline sensors should select those that can recognize high load conditions and either pass certain types of traffic without performing full analysis or drop low-priority traffic to reduce load. Another limitation of network-based IDSs is that they are susceptible to various types of attacks, most involving large volumes of traffic. Organizations should select products that offer features designed to make them resistant to failure due to attack.

Organizations should also ensure that IP addresses are not assigned to the network interfaces of passive or inline sensors used to monitor network traffic, except for network interfaces used for both traffic monitoring and managementKaren *Scarfone*. Peter *Mell*(2012). Network-based IDS sensors offer various prevention capabilities. Many passive sensors can attempt to end TCP sessions by resetting them, but this technique often does not work in time, and it is not applicable to non-TCP sessions, such as UDP and ICMP. Inline sensor-specific techniques include performing inline firewalling, throttling bandwidth usage, and altering malicious content, all of which are helpful for certain circumstances. Both passive and inline sensors can reconfigure other network security devices; they can also run third-party programs or scripts to initiate additional prevention actions*Scarfone*. Peter *Mell*(2012).

4. MULTI-COMPONENT INTRUSION ANOMALY DETECTION FRAMEWORK

The normal behavior of a computing system can be characterized by observing its properties over time. The objective of this system is detecting anomalies (or intrusions), it can be viewed as finding non permitted deviations of the characteristic properties in the monitored LAN network system. This assumption is based on the fact that intruders' activities in some way must be different from the normal users' activities.

In this section we are first presented with the objectives of the proposed system, its overall architecture, highlighting its four main components and the overall functioning. The important component of the proposed research is to analyze the computational aspects of the LAN network and integrate them in a single framework in order to develop a simple intrusion/anomaly detection and response system. Intrusion/Anomaly detection is an important part of computer security. It provides an additional layer of defense against computer misuse (abuse) after physical, authentication and access control.This design model is based on the hypothesis that an intruder's behavior will be noticeably different from that of a legitimate user, and security violations can be detected by monitoring network thresholds.For the purpose of this project only, we'll be focusing on parameters such as *system-level* parameters, *process-level* parameters and *Packet-level* parameters assuming that *user-level* parameters are being taken care of through other conventional authentication and access control methods.

The *system-level* parameters that provided indication of resource usage include

- Cumulative and per user CPU usage
- Usage of real and virtual memory
- Amount of swap space currently available
- Amount of free memory
- I/O and disk usage

Various *process-level* parameters monitored to detect intrusion are:

- The number of processes and their types
- Relationship among processes
- Time elapsed since the beginning of the process
- Current state of the process (running, blocked, waiting) and runaway processes
- Percentage of various process times (such as user process time, system process time and idle time).

Some of the parameters that are monitored to gather *packet-level* information:

- Number of connections and connection status (e.g. established, close_wait, time_wait)
- Average number of packets sent and received
- Duration of the connection
- Type of connection (Remote/Local)
- Protocol and port used

Historical data of relevant parameters are initially collected over a period of time during normal usage (with no intrusive activities) to obtain relatively accurate statistical measure of normal behavior patterns.

The four main components of this framework are;

i. Database Server
ii. Management Server
iii. IDS core system and
iv. A Sensor

- ❖ ***Sensor:***TheSensor monitors and analyzes activity on the network. It communicates with the management server and IDS to report an intrusion and it is also used to resolve the intrusion.
- ❖ ***Management Server:***The *management server* is the centralized device that receives information from the sensors and manages them. The management servers perform analysis on the event information that the sensors provide and can identify events that the individual sensors or agents cannot.
- ❖ ***Database Server:***The *database server* is a repository for event information recorded by sensors, agents, and/or management servers. Many IDSs provide support for database servers.
- ❖ ***IDS core system:*** The detection system monitors several parameters to determine the correlation among the observed parameters during intrusive activities. These observed parameters are used to determine a common resource threshold for each workstation on the LAN network.
- ❖ **User Interface:** Thisis a program that provides an interface for the IDS's users and administrators. Console software is typically installed onto standard desktop or laptop computers.

REFERENCES/BIBLIOGRAPHY/WORKS CONSULTED

1. Aickelin U, P Bentley, S Cayzer, J Kim, and J McLeod. Danger theory: The link between ais and ids. In Proc. of the Second Internation Conference on Artificial Immune Systems (ICARIS-03), pages 147–155, 2003.
2. Anita K. Jones and Robert S. Sielken , “Computer System Intrusion Detection: A Survey”, http://www.cs.virginia.edu/~jones/IDS-research/Documents/jones-sielken-survey-v11.pdf
3. Bace, R., Mell, P. 2001. Intrusion Detection Systems. Special Publication 800-31,National Institute of Standards and Technology (NIST).
4. Balasubramaniyan J.S, J. O. Garcia-Fernandez, D. Isacoff, Eugene H. Spafford, Diego Zamboni: An Architecture for Intrusion Detection Using Autonomous Agents. ACSAC 1998: 13-24
5. Biswanath Mukherjee, Todd L. Heberlein, and Karl N. Levitt, “Network Intrusion Detection”, IEEE Network, May/June 1994
6. ChandrashekharA. M and K. Raghuveer (2013), “Intrusion Detection Technique by using K-means, Fuzzy Neural Network and SVM classifiers”, International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, INDIA, (2013) January 4-6.
7. Chatzigiannakis V, G Androulidakis, M Grammatikou, B Maglaris. A distributed intrusion detection prototype using security agents, HP OpenView University Association
8. Chatzigiannakis V., Androulidakis G., Grammatikou M., Maglaris B. (2004) “A Distributed Intrusion Detection Prototype using Security Agents” Network Management & Optimal Design Lab (NETMODE), ECE Department – National Technical University of Athens (NTUA) Iroon Polytechniou str. Zografou, Athens, Greece.
9. Curry D. and H. Debar, “Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language(XML) Document Type Definition”, Internet Draft, November 2002.
10. Dhakar M. and A. Tiwari,(2012) “A New Model for Intrusion Detection based on Reduced Error Pruning Technique” International Journal of Computer Network and Information Security, (2013), pp. 51-57.
11. Dorothy E. Denning. An Intrusion-Detection model. In IEEE Symposium on Security and Privacy, pages 118--131, 1986
12. Heberlein L.T, K. N. Levitt and B. Mukherjee. A method to detect intrusive activity in a networked environment. In Proceedings of the 14th National Computer Security Conference, pages 362-371, 1991
13. Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J., Wolber, D. A network security monitor. In Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy. pp. 296-304. 1990.
14. Herve´ Debar, Marc Dacier, Andreas Wespi. Towards a taxonomy of intrusion-detection systems. Computer Networks 31 805–822. 1999
15. http://www.deic.uab.es/material/26118-capitol1.pdf
16. https://www.owasp.org/index.php/Intrusion_Detection as at 5th may 2016
17. J Boudec and S Sarafijanovic. An artificial immune system approach to misbehavior detection in mobile ad-hoc networks. Technical Report IC/2003/59, Ecole Polytechnique Federale de Lausanne, 2003.
18. James Brentano, Stephen R. snapp, Gihan V. Dias, Terrance L. Goan, KarnlN. Levitt, Biswanath Mukherjee, Stephen E. Smaha: An architecture for a distributed intrusion detection system. Division of computer science, University of California Davis, California 95616.
19. James Brentano, Steven R. SnappGihan V. Dias, Terrance L.Goan, Karl N. Levitt, Biswanath Mukherjee, Stephen E. Smaha (1991) “An architecture for a distributed intrusion detection system” Division of Computer Science University of California 95616

20. K Begnum and M Burgess. A scaled, immunological approach to anomaly counter measures (combining ph with cfengine). Integrated Network Management, pages 31–42, 2003.

21. Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (IDPS). Technical Report SP800-94, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, U.S. Department of Commerce, July 2012.
22. Karen Scarfone. Peter Mell.(2012) Special Publication 800-94. Revision 1 (Draft) ... Natl. Inst. Stand. Technol. Spec. Publ. 800-94 Rev. 1, 111 pages (Jul. 2012).
23. Marek Piotr Zielinski 2004: Applying Mobile Agents In An Immune-System-Based Intrusion Detection System; submitted in part fulfilment of the requirements for the degree of MASTER OF SCIENCE in the subject COMPUTER SCIENCE at the University Of South Africa
24. Marek Piotr Zielinski. Applying mobile agents in an immune-system-based Intrusion detection system. A dissertation submitted to the department of computer science, University of South Africa. November 2004
25. Mukherjee Biswanath, Todd L. Heberlein, and Karl N. Levitt, (1994) "Network Intrusion Detection", IEEE Network, May/June
26. P. R. Subramanian and J. W. Robinson, (2012)"Alert over the attacks of data packet and detect the intruders", Computing, Electronics and Electrical Technologies (ICCEET), IEEE International Conference on ISBN: 978-1-4673-0211-1, (2012) March 21-22, pp. 1028-1031.
27. S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J. Frank, J. Hoagland, K. Levitt, C. Wee, C. Wee, R. Yip and D. Zerkle. Computer Security Research Group. The Design of GrIDS: A Graph-Based Intrusion Detection System. Technical report, UC Davis, Dept. of Computer Sc., May 14, 1997.
28. Sanjay Sharma and R. K. Gupta (2015) "Intrusion Detection System: A Review." International Journal of Security and Its Applications, Vol. 9, No. 5 (2015), pp. 69-76 http://dx.doi.org/10.14257/ijsia.2015.9.5.07
29. Stephanie Forrest, Alan S. Perelson, Lawrence Allen, and Rajesh Cherukuri. Self-nonself discrimination in a computer. In Proceedings of the 1994 IEEE Symposium on Security and Privacy, page 202. IEEE Computer Society, 1994.
30. Steven R. Snapp , James Brentano , Gihan V. Dias , Terrance L. Goan , L. Todd Heberlein , Che-lin Ho , Karl N. Levitt , Biswanath Mukherjee , Stephen E. Smaha , Tim Grance , Daniel M. Teal , Doug Mansur, DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype, In Proceedings of the 14th National Computer Security Conference (1991)
31. Todd Heberline L, Gihan V. Dias, Karl N. Levitt, Biswanath Mukherjee, Jeff Wood, and David Wolber. (1990) A Network Security Monitor. In IEEE Symposium on Research in Security and Privacy, Pages 296--304, IEEE, May.
32. Uwe Aickelin, Julie Greensmith, and Jame Twycross (2004) "Immune system approaches to intrusion detection- a review" School of Computer Science University of Nottingham, UK.
33. WankhadeK., Patka S. and ThoolR., (2013) "An efficient approach for Intrusion Detection using data mining methods", International Conference on Advances in Computing, Communications and Informatics (ICACCI), Print ISBN:978-1-4799-2432-5 INSPEC Accession no. 13861274, August 22-25, pp. 1615-1618.
34. Yousef Farhaoui, Ahmed Asimi. (2012) "Creating a Complete Model of an Intrusion Detection System effective on the LAN",International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 3, No. 5.