Fighting against Intrusion using Behavioral Flow Level Anomaly Detection

Shraddha Saxena
Department of Information Technology
Samrat Ashok Technological Institute, Vidisha, India
saxena.29shra@gmail.com

Abstract— **Networking industry growing every month due to its attractiveness and the service to access from remote to remote in just a click. It also has dark side due to suspicious users and their modern weapons to launch attack on any network or system alone. There is a strong necessity to be protected from modern attacks using modern techniques. Also Computer Security has been a major issue over the past few years due to proliferation of internet in our life and the large set of services which it caters. Ease of servicing lead to the exponential growth of the Internet. The best way to prevent system from attack is to deploy never to deploy vulnerable software because in this case the lag time is significant between the announcement and the availability of a patch or a solution to fix the problem; this makes the job easier for misuse of resources. This paper provides an insight about intrusion, way of detection and how to prevent it using different methods. It also covers the pros and cons of the various security methods such as cryptography, firewall, IDS and IPS. And finally this paper presents a novel anomaly based Intrusion detection and Prevention System capable of detecting unknown types of attack like botnet, worms DoS, SYN and UDP FLOOD. Obtained results show that proposed mechanism is more promising and reliable than exiting. The beauty of the proposed approach is its simplicity and quick response to the unknown suspicious activity. For validating the effectiveness and response alertness it has been tested using HASDOSTESTER and HPING3 attack launching tools and it proofs it works well and produce satisfactory results which is higher than an existing one. Another thing is that it is working on the real time traffic flows rather than offline dataset. Soon it has been enhanced to detect Botnet and HTTP Trojan attacks.**

Keywords-Anomaly detection, Bot net, DoS, Hasdostester, HPING3, HTTP Trojan, Intrusion, Intrusion Detection and Prevention System (IDPS), SYN Flood, UDP Flood.

I. INTRODUCTION

Scariest of all, however, is the fact that, from phishing dodge to cyber-espionage, security threats continue to grow gradually, more sophisticated, complex, and difficult to detect and intercept. In today's world where Intruders are very smart and ingenious, it is not possible to identify all threat risks. So how can an organization proactively protect itself in such an environment? There is a strong need of security protection in modern communication systems.

Information or network security is defined as a practice of protecting data from illegitimate access, utilize, exposé, demolition, alteration, or disruption. It is concerned with ensuring that information related risks are assessed, appropriate controls are implemented to manage those risks, and that the adequacy of those controls are monitored on a regular basis.

According to [1], computer technology and Internet connections have essentially changed our style of life; various attacks over networks pose severe threats. A report by the Computer Security Institute [Richardson 2008b] showed that 32% of reporting organizations have been attacked by malware in 2008. As there is always a portion of computer users that do not install proper security systems, or neglect or unable to update their operating systems and/or security measures, their systems are more compromising to attacks? Breaching of the system may cause serious losses.

Vulnerability is a technical flaw or weakness in the design, implementation, or operation and management that can be exploited to violate a system security policy [ping et al. 2008]. Most of the vulnerabilities originate from software Vendors' design flaws. The vulnerabilities pose potential risks to users, and such risks are realized when they are exploited by network attacks.

Various methods have been used to protect the network and host from attacks like firewall, encryption and decryption and modern techniques. A firewall is a first line of defense it allows the authenticate packet and disallow other as fixed pattern matching. But it is unable to protect from modern intrusion attack. So there is need of another defense of line to be protected such as intrusion detection and prevention system (IDPS).

The rest of the paper organized as follow, section 2 describes related terminology and background work, and section 3 focuses on related work in IDPS and IPS field. Section 4 describes the proposed approach and the algorithm then section 5 discusses the results and the performance of the proposed system. And finally section 6 concludes of the article.

II. TERMINOLOGY AND BACKGROUND

According [2], there are both harmless and harmful users on the Internet. An organization makes information available to harmless Internet users, at the same time the information is available to malicious users as well. Malicious users or hackers can get access to an organization's internal systems in various reasons. These are often called Software bugs. Many factors impact the security threats to which a computer system is vulnerable. Naturally, some threats are more severe than others, so when trying to understand why an IPS is necessary in today's networks, you need to

consider the following factors- Technology adoption, Target value and Attack characteristics are:

Intrusion: Intrusion is an active sequence of related events that deliberately try to cause harm, such as rendering system unusable, accessing unauthorized information, or manipulating such information. This definition refers to both successful and unsuccessful attempts [3].

Intrusion Detection System: IDS can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. The intrusion detection part of the name is a bit of a misnomer, as an ID does not actually detect intrusions—it detects activity in traffic that may or may not be an intrusion [4].

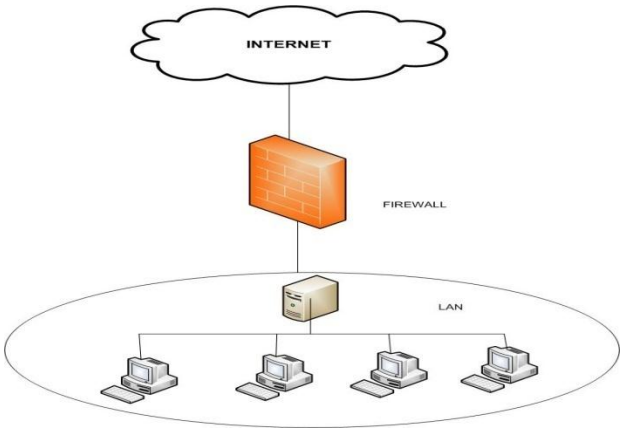

Fig. 1. Deployment of Firewall

II. (A) Firewall

The conventional method to secure the system i.e. First line of defense is Firewall. The firewall was most of what an administrator needed to protect a network from attack. It was easy to establish where your network ended and the Internet began.

In other words, Firewalls are usually the first component of any outside defense. Firewalls works as a barrier of security among networks of different levels of confidence or security, utilizing network level access control politics. The major functional requirement of a firewall is to protect a private (internal) network from unauthorized external access [5].

A firewall is governed by a set of rules or filters defined by the administrator [6]. A typical firewall will permit or reject incoming packets based on the port that the TCP or UDP request is arriving on. It is designed to refuse visibly suspicious traffic but is also designed to allow some traffic through. This behavior has a major disadvantage, as any packet is allowable through an open port in the firewall. Figure 1 shows the, how the firewall is working.

Many exploits take advantage of weaknesses in the very protocols that are allowed through the perimeter firewalls and once the web server has been compromised, this can often be used as a springboard to launch additional attacks on other internal servers [7]. Once a "rootkit" or "back door" has been installed on a server, the hacker has unfettered access to that server at any point in the future.

[8] Differentiate firewall, NIDS and NIPS, Firewalls filter undesirable traffic based on RULES (policies) to check packet headers. NIDS passively watch traffic on a network and perform more advanced checks, including inspection of protocols and its content, to determine indications of possible attacks. Network Intrusion Prevention Systems (NIPS) is the combination of NIDS and firewalls, performing in-depth inspection and using this information to block possible attacks.

II. (B) Types of IDS Systems

IDS and IDPS are the second line of defense. IDSs fall into one of three categories:

Host-based intrusion-detection system (HIDS): A HIDS system will require some software that resides in the system and can scan all host resources for their activity; some just scan SYSLOG and event logs for activity. It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base. Host-based technology examines events like what files were accessed and what applications were executed.

Network-based intrusion-detection system (NIDS): A NIDS system is usually in-line on the network, and it analyzes network packets looking for attacks.

Hybrids IDS: A hybrid IDS combines a HIDS, which monitors events occurring on the host system, with a NIDS, which monitors network traffic.

The biggest disadvantages of the majority of host-based systems HIDS is that they are passive, which means that they have to wait for an event to happen and cannot proactively prevent it. For example, if a system user (or a process) attains elevated permissions in an operating system as a result of intrusive actions, (or a Trojan) and is trying to destroy an important file, a passive system will detect a lack or modification of this file. A proactive system, in addition to notifying the system administrator, will also be able to prevent data from damage. This technique was used, among others, by the Linux Intrusion Detection System (LIDS) [9].

Intrusion Prevention System: An IPS sits in line on the network and monitors it, and when an event occurs, it takes action based on prescribed rules. This is unlike IDSs, which do not sit in line and are passive. Some people see IPSs as next-generation IDS systems, because they take detection a step further, but others think in broader terms and consider the IPSs to be yet another tool in the security infrastructure

that could help prevent intrusions. IPS has developed out of IDS, but they are really different security products that have different functionality and strengths. Fig2. Shows the general architecture of IDS and IPS with their respective positions.

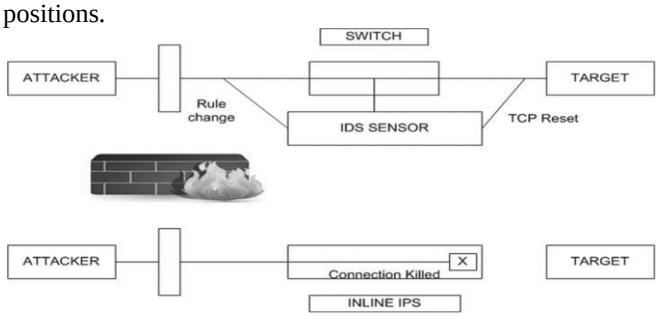

Fig. 2. Deployment of IDS and IPS in the network

IDS/IPS Attack Response: An IPS is an extension of a firewall and actively participates in access control and policy enforcement unlike IDS, which works off to the side and monitors what a firewall is missing. An IPS sensor sits on the wire intercepting and forwarding traffic flows, allowing them to kill attacks automatically similar to a firewall.

Types of IPS: Threre are three categories in which we can classify IPS (i) Host Intrusion Prevention System (HIPS), (ii) Network Intrusion Prevention System (NIPS), and (iii) Hybrid type.

A host-based IPS (**HIPS**), which work best at protecting applications, or a network-based IPS (**NIPS**). User actions should correspond to actions in a predefined knowledge base; if an action isn't on the accepted list, the IPS will prevent the action. Unlike IDS, the logic in an IPS is typically applied before the action is executed in memory. Other IPS methods compare file checksums to a list of known good checksums before allowing a file to execute, and to work by intercepting system calls.

Two methods are used to collect data on a switched network: Port mirroring and Network taps.

II(C). Common Detection Methodologies

Two well known methods used to detect and prevent the attack, Misuse and Anomaly detection or a hybrid of both. Misuse detection also called signature or rule based detection method.

1. **Misuse or Signature based IDS -** Misuse detection defines a set of "unacceptable" behaviors and alerts when system activities match this set [10]. Misuse detection looks for a specific attack that has already been recognized (Vulnerabilities and known attack patterns). Misuse detection recognized those types of attack which have known but new (unknown) pattern and characteristic of intrusion might not be identified using this technique [11] [12].
2. **Anomaly Detection based IDS -** Anomaly detection, works better to detect unknown attacks [13]. Anomaly detection believes that an intrusion will always reflect some deviations from normal patterns [14]. In Anomaly detector modeled a normal profile, if anything (network or behavior) deviated from normal treated as an anomalous behavior (or action). [13] Attacks like snooping network or abusing vulnerabilities in protocol's can be detected by analyzing header or traffic. But in case of the abusing by program vulnerabilities such as malcodes (worms or viruses) can't be handled by analyzing header information. Such types of attacks may be better detected by inspecting the packet payload (data field).

The fundamental necessities of an intrusion detector are efficiency and accuracy.

III. Related Work

Auditing of network data [14] is the first step required to detect intrusion, since the amount data that an IDS wants to scrutinize is very large even for a small network and extraneous feature on packets and network make it harder to identify suspicious activities in patterns [15].

The authors of [16] have demonstrated that a most of the features are insignificant and can be removed, without degrading the performance of the IDS [14]. Thus to make, an IDS to work efficiently and accurately in real time then it must diminish the amount of data to be processed.

Broadly IDS has divided into two types: host-based IDS (HIDS) and network-based IDS (NIDS) [17]. Host-based IDSs [18] [19] detect intrusions by examining file system modifications, application execution logs, system calls, and so on; while network-based IDSs detect intrusions by monitoring packets that pass through on network links.

Compared to network-based IDSs, host-based IDSs have access to more refined resources, such as file system and system calls. On the other hand, network-based IDSs are able to detect intrusions at an earlier stage and they have global views of the networks. As a result, these two systems can complement each other to provide high quality detection.

One important point to keep in mind before making as IDPS is FALSE NEGATIVE and FALSE POSITIVE [20]. Ying-Wei Kuo and Shou-Hsuan Stephen Huang [20] suggest, False negative signify that an ATTACK is mistakenly treated (classified) as a NORMAL one, while the false positive signify a NORMAL packet (data/connection) is declared as an ATTACK.

According to the technology IDS broadly divided into categories Host based and Network based.

NIDS is an essential tool to secure network [21] that automate detection by gathering data from medium and perform analysis those data to find intrusion, if found any threats or unusual behaviors then, it reports and alert by

message to administrators. A NIDS might also provide automatic responses to those security attacks in case of it integrate the with Prevention mechanism.

The major weakness of NIDS is having false positives. Noise is another type of false that can severely limit the effectiveness of NIDS. The NIDS sends an alert on a condition that is non-threatening or not applicable to the site that is being monitored. In this case, the NIDS diagnoses the situation correctly and does not make any mistake but the alarm is of questionable value [22]. False positive alarms and noises can annoy the administrator since they are not real attacks or security threats.

Some problems revealed by [23], showed the insufficiency of information obtained from the wire that can cause noise and NIDS vulnerability to evade attacks. Another issue in NIDS research [23] considers about the flexibility of signature and policy that makes NIDS more accurate.

For solved these problem Author [21] proposed a new solution to SNORT NIDS, named target-based IDS. Author [21], suggests the solutions for reduction of noises. Proposed NIDS diagnose the packet stream in the same perspective as the host does. The proposed scheme has used the concept of dynamic policy to enhance the performance of SNORT [10]. Transformation of firewall information via the network is an issue that results performance lacking of SNORT NIDS.

Several IDS methods have been proposed; some of them are based on the ideas of the human immune system [24]. Such as positive or negative characterizations [25] [26] [27] [28]. D. Dasgupta [29] has contributed great work in the field of Artificial Immune System (AIS) and its application in the field of Network Security.

Author of [30], suggest the characteristics of a good IDS. He said that, an idyllic IDS offers a high attack detection rate, low detection delay and low false positive rate, but in practice this is hard to achieve. The detection rate is calculated as the fraction of the number of correctly detected attacks to the total number of attacks, whereas the false alarm rate is figured as the ratio of the number of normal connections (that is incorrectly misclassified as attacks) to the total number of normal connections.

Author of [2] has depicted that, Advantage of Anomaly detection over misuse is that, it can detect unknown attacks and privilege abuse of legitimate users as well. Authors of talked about the application level anomalies most often used by today's attackers to target the vulnerabilities of specific systems or applications as mentioned in. Another advantage of anomaly detection is to defense against Zero-day attack [31].

IV. PROPOSED APPROACH

In this section, the proposed approach has been discussed based on anomaly detection and it is the core thing algorithm has two steps first is to detect common attacks (using the anomaly Detector engine) and a second phase is designed to detect bot attack.

Our proposed working system fighting against intrusion using flow level anomaly uses anomaly detection concept to detect unknown attacks on determining using real time traffic (flow). Proposed system has following attractive features –

1. The proposed solution is the enhancement of the base paper [2] its provide a better and faster response to the intrusion and defense against new (unknown) attacks.
2. Another beauty of the proposed solution is it can detect and prevent modern types of attacks like DoS, SYN Flood, UDP Flood Worms and Bot Attacks too.

Following problem has been identified in base paper [2]-

1. The Author has used the concept of Agent, it increases the computation overhead.
2. The second important issue is the overhead of agent management and security issues (author as discussed in future work).
3. Last but not the least is author's article does not talk about any specific attack of the modern era like DoS, SYN Flood, UDP Flood and Botnet attack.

Proposed Algorithm - I:

1. The record flows (network traffic) and stored into database as described in [2].
2. Calculate Mean, minimum, maximum and average of traffic.
3. Then calculate a threshold value say Tv calculated as the mean value over the last 20 minutes plus/minus five times its standard deviation.
4. Calculate TCP work weight: (0..100%)
   IP src: S(s) + F(s) + R(r)/total pkts
5. Validation Phase- In this phase the behavior of packet or user (say V (variable)) have been compared with Tv.
6. Our Anomaly Detector calculates following to check anomaly:
   a. TCP work weight:
      IP source: (syn +fin + reset)/total pkts
   b. TCP worm weight:
      IP src: syn - fin > N
      Where N number of control bits. We have fixed its value to *18.
   c. TCP error weight:
      IP src: (syn - fin) * (reset+ICMP_errors)
   d. UDP work metric:
      IP src: (UDPs – UDPr) * (ICMP_errors)

After that all these four metrics have compared with threshold (Tv) and check the deviation if found and raise alert.

Proposed Algorithm– 2
(Method of Detecting HTTP Trojan/ Bot)

1. For (all traffic (incoming/ outgoing) do:
   Collect real time traffic as flow statistics
   TOTAL network traffic capture
   DNS statistics
   TCP Traffic and SYN count
   TCP traffic with PUSH flag
   UDP Traffic
   HTTP traffic on port 80
2. If (traffic capture > average or DNS > average) then
   Calculate TCP work weight (as proposed in main PROPOSED ALGORTIHM):

Else if (UDP work weight >70)
{
Msg ="HTTP Trojan is detected"
Raise the alert
BLOCK IP address of the suspicious traffic
RESET (using TCP RESET) the connection
Send ICMP unreachable msg to attacker
}

V. RESULTS AND PERFORMANCE

The proposed behavioral approach has been developed on real time traffic (flows) on Ubuntu system and real time traffic has been captured where proposed method has been validated.

To achieve this following setup has been followed-

1. Deployed and developed – Ubuntu 13.04 has been chosen to deploy proposed security system for better and accurate measure of security system using ourmon [2]. To validate and determination of anomaly (real-time traffic to ADE) JAVA has been applied as a middleware.
2. Knowledge Base – Round robin database has been used.
3. Validation and testing – For checking the working and response time of the proposed system attack has been launched from different machines (LAN may be or not same) and target on the proposed IDS. The following tools have been used to launch the attack for validating the accuracy and detection rate of the proposed method deployed on an Ubuntu 13.04 system-
   (a) Hasdostester [32] –This tool has been used to launch DoS (denial of service) attack.
   (b) Hping3 [33] – To launch SYN and UDP flood attack.

The beauty of "Hasdostester" tool is that is easy to launch and due to Java based it can run from any platform. We have launched the attack from windows 7 PC to Ubuntu.

Another tool which has been referred for testing of detecting SYN and UDP flood attack is open source "HPING3" famous amongst security professional. Hping3 is easy to use and install on Linux systems.

For this another Ubuntu system has been prepared and to penetrate the proposed system via the same network (LAN), then SYN and UDP attack has been launched towards a targeted system (Proposed System) on which the proposed IDS has been deployed with varying number of packet sizes. The obtained results show that the proposed system works better and has a faster response to the newly and known attacks due to the its core concept i.e. Anomaly detection.

Results-

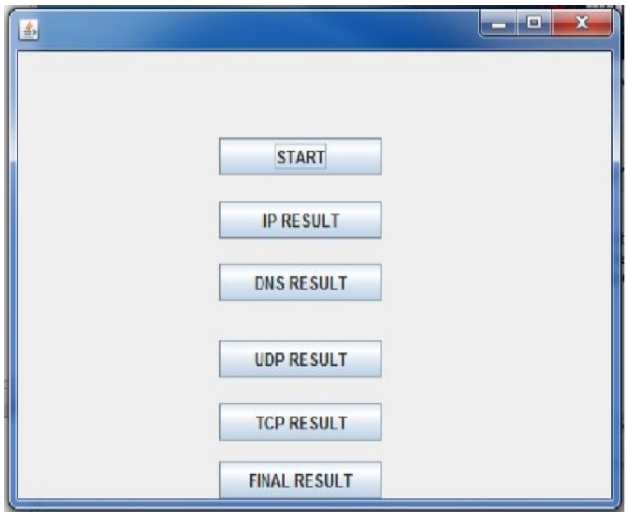

Fig. 3. Home screen of Proposed IDS

Figure 3 shows the proposed system home screen developed using Java language that interacts with real time traffic and response the various attacks has been detected and gives the option to the administrator to choose the appropriate action against them in the network and the host both (depending on the choice where the proposed has been deployed).

Number of TCP worms: As shown in the table 3 proposed system caught following TCP worms attack with their relative frequency on which take has been detected.

Table 3. Number of TCP Worms

S.No	IP Address Caught	Date and Time	Frequency
1.	172.16.14.96	Tue Jul 9 12:22:36 IST 2013:	400
2.	172.16.14.35	Thu Jul 25 10:55:03 IST 2013	443

3.	172.16.1.1	Thu Jul 25 14:10:35 IST 2013	1511
4.	172.16.14.25	Thu Jul 25 10:58:04	441
5.	192.168.1.1	Mon Jul 22 15:17:09 2013	200

Number of UDP Floods: As shown in the table 4 proposed system caught following UDP flood attack with their relative frequency on which take has been detected.

Table 4. Number of UDP Flood

S.No	Date and Time	IP Address Caught
1.	Fri Jul 12 18:33:01 2013	192.168.0.1
2.	Fri Jul 19 21:12:02 2013:	192.168.0.101
3.	Fri Jul 19 00:02:32 2013	14.139.232.5
4.	Mon Jul 22 19:02:40 2013	91.189.94.4
5.	Fri Jul 19 09:02:32 2013	172.16.14.135

Number of Intrusion Detected: Table 5 shows the total number of intrusion detected by the system till date. And will collect many more.
The intrusion has been caught on the basis of the proposed mechanism in which anomaly detection on the real time flows has been applied.

Table 5. Number of Intrusion Detected

S. No	Date and Time	IP Address Caught	Freq.
1.	Tue Jul 9 12:22:36 IST 2013:	172.16.14.96	400
2.	Thu Jul 25 10:55:03 IST 2013	172.16.14.35	443
3.	Thu Jul 25 14:10:35 IST 2013	172.16.1.1	1511
4.	Thu Jul 25 10:58:04	172.16.14.25	441
5.	192.168.1.1	192.168.1.1	200
6.	Fri Jul 12 00:00:01 2013	192.168.0.101	395
7.	Fri Jul 19 21:12:02 2013:	115.118.0.182.static-ttsl-hyderabad.vsnl.net.in	300
8.	Fri Jul 12 00:02:32 2013	OCSP.TKO2.VERISIGN.COM (199.7.57.72)	25
9.	Fri Jul 26 00:02:32 2013	192.168.0.103	400
10.	Fri Jul 19 09:02:32 2013	172.16.14.135	600
11.	Fri Jul 19 21:41:34 2013:	176.31.236.210	1
12	Fri Jul 26 19:42:01 2013	maa03s16-in-f6.1e100.net(74.125.236.166)	20
13.	Sat Jun 15 00:00:34 2013:	airtelbroadband.in(122.175.190.48)	20
14.	Fri Jul 12 18:33:01 2013	192.168.0.1	1
15.	Fri Jul 19 21:12:02 2013:	192.168.0.101	2
16.	Fri Jul 19 00:02:32 2013	14.139.232.5	3
17.	Mon Jul 22 19:02:40 2013	91.189.94.4	1
18.	Fri Jul 19 09:02:32 2013	172.16.14.135	2

VI. CONCLUSION

Global internet is increasingly pervasive; IDS/IPS has a major role to play in the domain of computer security. This article surveyed the current security mechanism like firewall IDS and IDPS and their methods. It has been proved that anomaly detection works under unknown and zero days'. This paper presents a novel anomaly based Intrusion detection and Prevention System capable of detecting unknown types of attack like Botnet, worms DoS, SYN and UDP FLOOD. Obtained results show that proposed mechanism is more promising and reliable than exiting. The beauty of the proposed approach is its simplicity and quick response to the unknown suspicious activity. For validating the effectiveness and response alertness it has been tested using HASDOSTESTER and HPING3 attack launching tools and it proofs it works well and produce satisfactory results which is higher than an existing one. Another thing is that it is working on the real time traffic flows rather than

offline dataset. Soon it has been enhanced to detect Botnet and HTTP Trojan attacks. In the future, we can also deploy our AIPS in a distributed environment.

REFERENCES

[1] Jingguo Wang, Nan Xiao and H. Raghav Rao "Drivers of Information Security Search Behavior: An Investigation of Network Attacks and Vulnerability Disclosures", ACM Transactions on Management, Information Systems, Vol. 1, No. 1, Article 3, Publication date: December 2010.

[2] Rathore, J.S. , Saurav, P. and Verma, B. "AgentOuro: A Novelty Based Intrusion Detection and Prevention System", IEEE, Fourth International Conference on Computational Intelligence and Communication Networks (CICN), pp. 695-699, 2012.

[3] Igor Kotenko and Mihail stepashkin "Analyzing Vulnerabilities and Measuring Security Level at Design and Exploitation Stages Computer Network Life Cycle" Computer Network Security ,Third International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, MMM-ACNS 2005, St. Petersburg, Russia, September 24-28, 2005. Proceedings.

[4] Earl Carter and Jonathan Hogue "Intrusion Prevention Fundamentals", CICCO PRESS, 2006.

[5] Christopher W. Geib and Robert P. Goldman "Plan Recognition in Intrusion Detection Systems", IEEE, 2001.

[6] Liu Jianxiao and Li Lijuan "Research of Distributed Intrusion Detection System Model Based on Mobile Agent", IEEE, International Forum on Information Technology and Applications, 2009.

[7] Sheng SUN and YuanZhen WANG "A Weighted Support Vector Clustering Algorithm and its Application in Network Intrusion Detection", IEEE, First International Workshop on Education Technology and Computer Science, 2009.

[8] Konstantinos Xinidis, Ioannis Charitakis, Spiros Antonatos, Kostas G. Anagnostakis, and Evangelos P. Markatos "An Active Splitter Architecture for Intrusion Detection and Prevention", IEEE Transactions On Dependable And Secure Computing, Vol. 3, No. 1, January-March 2006.

[9] Jack Koziol, "Intrusion Detection with Snort", SAMS, 2nd Edition of Book, May 2003.

[10] Jung Yeop Kim and Rex E. Gantenbein "Automated Anomaly Detection Using Time-Variant Normal Profiling", World Automation Congress (WAC), Budapest, Hungary, July 24-26, 2006.

[11] Faizal, M.A., Mohd Zaki M, Shahrin Sahib, Robiah, Y., Siti Rahayu, and S., 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.

[12] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S" Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions" In Proceeding of CCS ACM Conference, 2002.

[13] Irfan Ahmed,and Kyung-suk Lhee "Detection of malcodes by packet classification" , The Third International Conference on Availability, Reliability and Security,IEEE,2008.

[14] V´aclav Sn´a˘sel, Jan Plato˘s, Pavel Kr¨omer and Ajith Abraham" Matrix Factorization Approach for Feature Deduction and Design of Intrusion Detection Systems", the Fourth International Conference on Information Assurance and Security, IEEE, 2008.

[15] W. Lee., S. Stolfo. and K. Mok,"A Data Mining Framework for Building Intrusion Detection Models", Proceedings of the IEEE Symposium on Security and Privacy, 1999.

[16] H. Sung and S. Mukkamala"Identifying Important Features for Intrusion Detection Using Support Vector Machines and Neural Networks", Proceedings of International Symposium on Applications and the Internet (SAINT 2003), pp. 209-217, 2003.

[17] H. Debar, M. Dacier, and A.Wespi. Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8):805{822, 1999.

[18] D. E. Denning "An Intrusion-Detection Model", IEEE Transactions on Software Engineering, Volume SE-13, No. 2, pp.222-232, 1987.

[19] T. F. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. L. Edwards,H. S. Javitz and Al Valdes, "IDES: The Enhanced Prototype - A Real-Time Intrusion-Detection Expert System", Computer Science Laboratory, SRI International, Menlo Park, CA, Number SRI-CSL-88-12. 1988.

[20] Ying-Wei Kuo and Shou-Hsuan Stephen Huang "An Algorithm to Detect Stepping-Stones in the Presence of Chaff Packets", 14th IEEE International Conference on Parallel and Distributed Systems, 2008.

[21] Mati Pinyathinun and Chanboon Sathitwiriyawong "Dynamic Policy Model for Target Based Intrusion Detection System", ACM, ICIS, 2009.

[22] Ranum, M. J. 2003. False Positives: A User's Guide to Making Sense of IDS Alarms, ICSA Labs IDSC.

[23] Ptacek, T. and Newsham, T. "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection System", Technical Report, Secure Networks, Inc, 1998.

[24] Alexander Krizhanovsky and Alexander Marasanov "An Approach for Adaptive Intrusion Prevention Based on the Danger Theory", Second International Conference on Availability, Reliability and Security (ARES'07), IEEE, 2007.

[25] U. Aickelin and S. Cayzer, "The Danger Theory and Its Application to AIS", Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS-2002), 2002, pp. 141-148.

[26] D. Dasgupta and F.A. Gonzalez, "An Immunity-Based Technique to Characterize Intrusions in Computer Networks", IEEE Transactions on Evolutionary Computation, 2002, pp. 1081-1088.

[27] F.A. Gonzalez and D. Dasgupta, "Anomaly Detection Using Real-Valued Negative Selection", Journal of Genetic Programming and Evolvable Machines, April 2003, pp. 383-403.

[28] A. Somayaji and S. Forrest,"Automated Response Using System-Call Delays", Proceedings of the 9th USENIX Security Symposium, 2000.

[29] Dipankar Dasgupta, http://www.msci.memphis.edu/~dasgupta/

[30] Farah Barika KTATA, Nabil EL KADHI and Khaled GHEDIRA "Distributed agent architecture for intrusion detection based on new metrics", IEEE, Third International Conference on Network and System Security, 2009.

[31] KDD09. INTRUSION DETECTOR LEARNING [EB/OL]. .http://kdd.ics.uci.edu/databases/kddcup99/task.html, 2010-09-19.

[32] Hasdostester tool, available at http://keralacyberforce.in/hash-algorithm-collision-dos-attack-with-xenotix-hash-dos-tester/.

[33] HPING3 , http://linux.die.net/man/8/hping3