

TAXONOMY BASED INTRUSION ATTACKS AND DETECTION MANAGEMENT SCHEME IN PEER-TO- PEER NETWORK

Prashant Kumar Singh¹
(prashant.mngr@gmail.com)

A. K. Vatsa¹
(avimanyou@rediffmail.com)

Reetu Sharma²
(reetuusit@gmail.com)

Priyanka Tyagi³
(pp.priya05@gmail.com)

¹Shobhit University, Meerut, UP, India.

²CERT, Meerut, UP, India,

³DVSIET, Meerut, UP, India,

Abstract : *A intrusion provides an unauthorized access, damage or disruption of the network. The process can understand the characteristics and nature of an intruder. The paper presents the taxonomy consists of the specification of an intruder. Taxonomy provides the classification of intruder and provides mechanism for intruder detection. We found the algorithm for developing an intruder which can be attack at host system or network system. Here provide the mechanism for an intrusion by using the system attribute and detection mechanism is based on knowledge and behavior of the system. Intrusion-detection mechanism using pattern based and threshold based mechanism for detecting an intruder. An intruder continuously monitored the network and host activities for detecting attack into the network and the task of intrusion-detection is also monitor the usage of such systems and detects the apparition of insecure states.*

Keyword : Intruder, Taxonomy of attack, Intrusion detection, Intrusion Attacks, Peer-to-peer network.

1. INTRODUCTION:

A network has different types of activities over the network and these activities could be trace by an intruder or attacker. An intruder matches all these activities over the network and access into the network. Intrusions have included preventive design issues, configuration files, and operational techniques to construct intrusion difficult. In Peer to peer network many system are connected and these systems have host id, source and destination address protocol. An intruder will attack at the system information like log file, data file and configuration file etc

A network grows and expands, it has become a many types of intrusion can attack [1] over the network and also apparent that more and more possibilities for miscommunication to occur between connections. The Packets of information overload the system information, identified user in gaining accesses to database files, miss-configure the devices, networks slowdown and etc. These complexities have created a demand for a sophisticated means to analyze the traffic and security level of network. Network-based intrusion detection [6] can monitors the entire, wide network with a few well-maintain nodes or different devices and impose the less overhead on the network. Network-based Intrusion detection is not mostly active devices that monitor ongoing network activities without interfering into the network operation. They have easy to secure through attack [12] and might even be no detectable to attacker; it has also required too little effort to installation and use into existing networks.

Taxonomy is defined as to study about general aspects of technical classification. The taxonomy word is used to express the actual hierarchy or classification of many objects. This classification is provides according to the relations about the characteristics of the different objects. Taxonomy is providing useful and important issues for study” [6]. The collection is useful when it is classified based on set of rules [7]. As suggested in the introduction, taxonomies of vulnerabilities might be useful in the security assessment process. The information can provide for designers or developers to left the building features. Vulnerability taxonomy also provides the way of exploring unknown attacks [8]. A leaf node or subdivisions into the taxonomy are represents a potential exploits. If the taxonomy has a grading system that can designate vulnerabilities according to their criticality, it can help prioritize the resources of the defense team [4]. In order to help disseminate knowledge of new vulnerabilities and attacks, many security organizations maintain central databases of vulnerabilities.

The taxonomy of attacks has been proposed over many years, but here still no standard accepted taxonomy. There are various analyzing techniques [9], counting through support vector machines, or use of expert systems and data mining, has been already used as a part of the detection process.

The difficulties will be exactly declaration of an attack. The taxonomy’s aim to increases the comparison of intrusion process. The taxonomy provides many types of outputs that can be generated by the intrusion systems, which is also, used the types of information used to find the intrusion. Security assessment of a system is the process of determining the system’s capability to resist attacks. This process involves to probing the system to detect the known vulnerabilities.

This paper is organized as follows: In Section 2 we present purposed works. In section 3 we present taxonomy based intruder, detection and prevention. Section 4 presents the conclusion, section 5 presents future scope and section 6 present references.

2. BACKGROUND

Most of works on attack taxonomies finds their goals, its properties, and its dimensions to classification and their suitable aspects for the use in a security process. In [17] developed a two-dimensional matrix of computer attacks. These are consisted of many types of users that are developers, operators, intruders, data entry, internal users and external users. Another dimension included the types of crimes that are kept the services, physical destruction, destruction the knowledge, browsing history and more. The types of users in the context of an attack also represent the source of an attack.

The class internal users are similar to the class’s operators, programmers, and data entry. A class for external users is similar to the intruder’s class. The taxonomy would have been more useful if these categories were either further refined into a hierarchical taxonomy or were grouped into a common higher-level category.

There are the different types of system crimes that are equivalents to the results of an impact or attack. Every attack represents the results of an attack or intrusion. They presented a two-level hierarchical classification. In the first level they presented four types of attacks:

- Theft of computer resources
- Disruption of computer resources
- Unauthorized disclosure of information
- Unauthorized modification of information in a computer

Although there is a two-level hierarchy, the second level was not clearly distinguished. The six types in the second level were jointly put under two categories of the first level. As

noted in [15], the authors of [18] probably did not intend to build taxonomy. They were merely attempting to list all possible types of misuse techniques.

Characterizing an attacker, if there is a good description of an attacker available the prediction of the course of action is much more precise and the already compromised devices are more easily identified. Here find the knowledge about an attacker? And the answer should collect all possible information about an intruder, so that one can describe him. First of all, everything, what the intruder has already done, should be observed. This includes the attacks and how he uses the devices and the data he has access to. [3] Suggests the attacks can be partly described by watching the following attributes:

Occurrence of activity, Patterns of behavior, e.g. time, tactics or network access, Network activity: sources, destination addresses, the path taken, Devices accessed: hardware, operating system, servers and applications, Data accessed, Tools and techniques used, Files left on systems, Information that can be used for intrusion-detection, Degree of success, Type of security compromised: confidentiality, integrity, availability, Vulnerability compromised, Exploits used.

Taxonomy elements: There are a number of concepts we use to classify intrusion-detection systems presented in Figure 2.1.

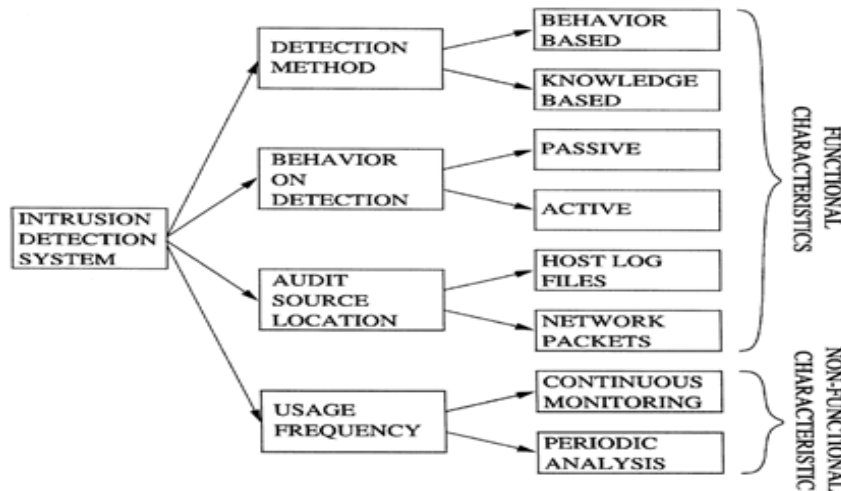


Figure 2.1: Characteristics of intrusion-detection systems

The behavior of detection provides the response of intrusion-detection system for possible attacks. When it actively reacts to the attack by taking either corrective (closing holes) or proactive (logging out possible attackers, closing down services) actions, then the intrusion-detection system is said to be active. If the intrusion-detection system merely generates alarms (including paging, etc), it is said to be passive. The input information can be audit trails, system logs or network packets.

Usage frequency is an orthogonal concept. The first three elements are grouped in the category “functional characteristics” because they refer to the internal workings of the intrusion-detection system, namely its input information, its reasoning mechanism, and its interaction with the information system. The scanners are sometimes attached to the intrusion-detection area, and we must differentiate discriminate between them and “real” intrusion-detection systems.

3. PROPOSED WORK

3.1 Architecture of taxonomy based intrusion detection management scheme in peer-to-peer network

The proposed mechanism of an Intruder based on taxonomy and provides detection mechanism for this intruder. The architecture for the proposed intruder is as follows:

1.2 Intruder based taxonomy

In this taxonomy presents the characteristics and specification of an intruder. It affects the host system and network. Various classification criteria are illustrated in figure 3.1.

❖ Types of Intruder

The taxonomy presents two types of intruder that is a host based intruder and network based intruder.

- **Host-Based intruder**

Use host system information to attack. It is categorized into OS based and network based. It has the following attribute.

❖ OS based attribute

This taxonomy provides the different types of attribute which is classified again into, file system and memory management. The file system has attributes like metadata values and different APIs. Memory management has allocator files, the garbage value which is collected in ITable.

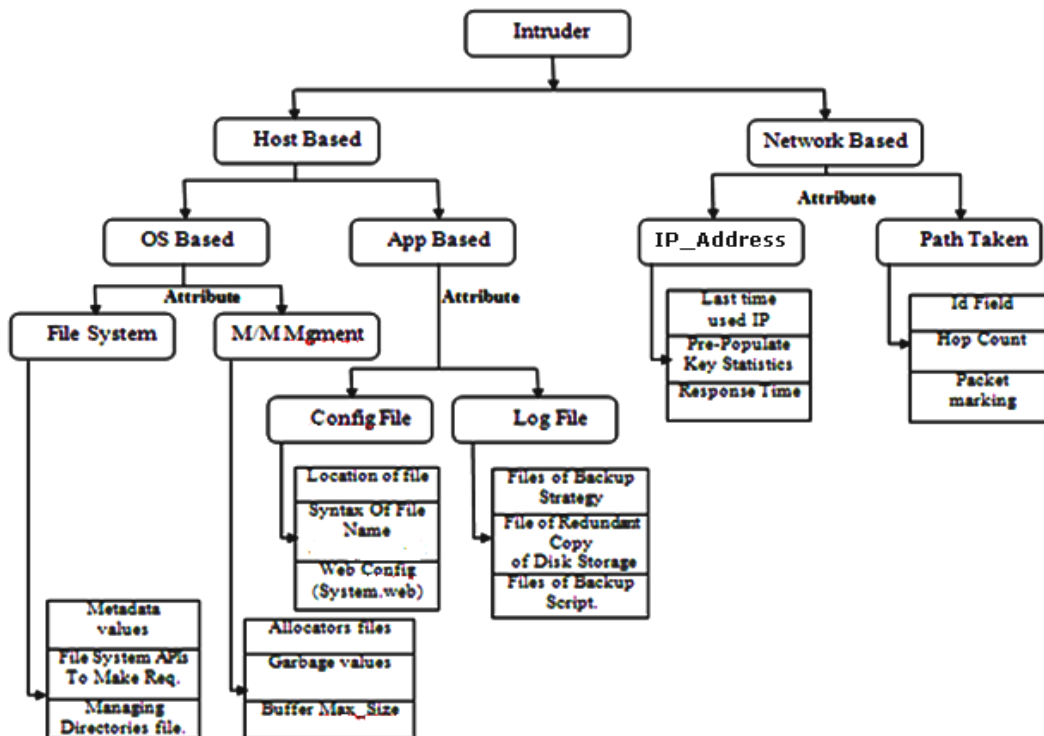


Figure 3.1: Intruder Based Taxonomy

❖ Application based attribute

The application based attribute classified into configuration file and log file. These files are used by the host system. The log file consists of the file of backup strategy, and copy of disk storage file. Use configuration file which has the information about location of file, syntax of file name etc.

3.1 Network-Based intruder

The network based intruder provides attack on network. It has the two types of attribute that are IP address and Path taken over the network. These attribute has different types of attribute which is stored into the ITable.

Architecture of IP attack

The Architecture presents the taxonomy of an attack over the network and host system. In figure 3.2 an attack is performing on destination IP address by an intruder and this attack is known as IPAddress attack. The following architecture of an intruder attack:



Figure 3.2: IP address attack

An intruder can attack at source_IP address and port_IP address. In figure 3.2 shows the attack to destination IP

3.2 Mechanism of Taxonomy based intrusion detection and prevention management scheme

The proposed mechanism is discussed into two phases

Phase - I: Taxonomy based Intruders:

The taxonomy based attack is categorized into two types like Host based and Network based intruder.

Type – 1: HostBasedIntruder

```

HostIntruderAttacks()
{
    • GetHostAttribute ( );
    • Store all attributes parameters in ITable (Intrusion table).
    • Match activities and behavior of host according to parameters stored in the ITable.
    • Thereafter, Intruder tries to harm, stop and affect the activities of host by changing
      the parameters values of host system.
}
GetHostAttribute()
{
    Case -1: OS_BasedIntruder
    {
        FAccessControl() // Intruder use FAT file system.
        {
            • Intruder collects following taxonomy information from FAT file
              system that information stored in ITable.
            • FAT file system consist of file system APIs to make requests, metadata
              value, managing directories file.
        }
        FAccessAttack( ) // If an attack occurs then an intruder matches these
                          parameter with ITable.
        {
            If (directories file is matched with attribute (directory) of ITable)
    
```

```

    Intruder exists into the host;
    Else
    Not exist into system;
    }
MemoryMgmnt( ) // Intruder access into memory to read the file
                    information.
    {
    • Intruder use the taxonomy of memory management activities that
      consist of allocator files, garbage values and buffer MaxSize.
    • An intruder collects used garbage values of host and stored it into the
      ITable.
    }
MemoryMgmntAttack( ) // Intruder tries to matches the garbage value of
                        host system from ITable.
    {
    If (garbage_value (Host) = Attribute of ITable)
    Intruder exists into host system;
    Else
    Failed to exist;
    End ( );
    }

```

Case-2: ApplicationBasedIntruder

```

{
ConfigurationApp( ) // Intruder used the configuration details.
    {
    • Collect configuration detail from host system that consists of file
      location, syntax of file (like file specifier (//) or client syntax (/)) and
      web config file (like system.web).
    • An intruder found these details through web or sharing information
      through web pages and stored it into ITable.
    }
ConfigAppAttack ( ) // an intruder attack through web and match the details
                        of configuration file from ITable.
    {
    If (specifier matches = attribute of ITable)
    Intruder existence successfully;
    Else
    Intruder existence failed;
    End ( );
    }
SystemLog( ) // It comes from the device changes, system changes,
                events and operations followed by the user.
    {
    • Taxonomy consists of log files that contain the files of backup strategy,
      redundant copy of disk storage and backup scripts.
    • An intruder collects of these parameters and stores it into ITable for
      further processing.
    }
SystemLogAttack( ) // an intruder attack and tries to matches these
                        log files from ITable.
    {
    If (File of backup script= attribute of ITable)

```

```

        Successfully exist;
        Else
        System existence failed;
        End ( );
    }

```

Attributes of ITable

- ❖ Various attributes like
 - File system,
 - Memory management,
 - Configuration file
 - Log files

Architecture of ITable (Host based)

File_system	M/m_mgment	Config_file	Log_file
Metadata values	Allocator files	Location of file	Files of Backup Strategy
File System APIs To Make Requests	Garbage values	Syntax Of File Name (file Specifier)	Files of Redundant Copy Of Disk Storage
Managing Directories file.	Buffer MaxSize	Web Config (System.web)	Files of backup Script.

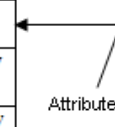


Table 3.1: Architecture of ITable (Host based)

Type – 2: Network Based Intruder

```

IntruderAttacks()
{
    • GetNetworkAttribute( )
    • Store all attributes parameters in ITable (Intrusion table).
    • Match activities and behavior of host according to parameters stored in the ITable.
    • Thereafter, Intruder tries to harm, stop and affect the activities of host by changing the parameters values of host system.
}

GetNetworkAttribute( )
{
    IPAddress( ) // contains the address and knowledge about source and destination host system.
    {
        • Network based taxonomy consist IP address that comes from Locator and other DNS tools.
        • An intruder collects an IP address to determine the last time used an IP address, pre-populate key statistics like DNS, response time and stored these details in ITable.
    }
    IPAddressAttack( ) // an intruder attacks the network and tries to match this parameter from ITable.
    {
        If (last time used IP matched with Attribute of ITable)
        Successfully enter into network;
        Else
        Failed to enter;
    }
}

```

```

End();
}
PathTaken() // path taken by Packets between host to host across an IP
            network.
{
    • An intruder collect the parameters from path taken by packet that use
topologies, packet marking, ID field, Hop count and stored it in ITable.
}
PathTakenAttack() // attack by an intruder into the network and match these
                  parameter from ITable.
{
    If (Marking packet matched with attribute of ITable)
    Successfully exist;
    Else
    Failed to exist;
    End();
}

```

Attribute of ITable

- ❖ Attributes are
 - IP address
 - Path taken over network

Architecture of ITable (Network based)

Ip_Address	Path_Taken
Last Time used IP	Id Field
pre-populate key statistics like DNS	Hop Count
Response Time	Packet Marking

Table 3.2: Architecture of ITable (Network based)

Initialization of ITable

- Initialize the attribute in ITable.
- An intruder used ITable’s attributes to match with host system and network activities to crack system.
- If intruder found activities of system or network which will be matched with attribute of ITable then exist into the network or system.
- If any activities of the system or network will not matched with attribute of ITable then follows the update process.
- Update process provides adding of new attributes in ITable for further accessing.

Access/Attack by an Intruder:

```

IntruderAccess()
{
    • Source sends information over the network to the destination address.
    • When a sequence of packets are arrival in the network, an intruder track the source
or destination IP address, counting the hop or path taken over the network, by
matching with attributes of ITable.
    • Tracking the above activities of the network and access into the network is known
as the network based intruder.
}

```


- If found host based activities that are when user done any activities at the system, then system could be creates log files, file system, Memory management and configuration file.
- A host based intruder match all these parameter with attribute of ITable and track the system or exist into the system.

}

Phase II: Detection mechanism

Intrusion detection is to detect every attempted intruder or DDoS attack as early as possible and to have a low degree of false positives.

- The detection mechanism provides the detection method for an intruder.
- When an intruder tries to attack or read IP address of the system, then a detection mechanism is used to detect this attack.

The following types of detection mechanisms are:

❖ Detection using pattern

DetectionPattern()

{

- For attack, an intruder uses the system information like File system which consists of File system APIs, update metadata & positioning etc.
- Detection technique creates patterns of all consisting file system in ITable and store in IDB (Intrusion Database).

}

DetectionPatternAccess() // when attack occur, the parameters of an intruder match with stored patterns in IDB.

{

If (parameters of intruder matches with patterns stored in IDB)
 Detect the intruder;
 Else
 detection failour;
 Update IDB;
 Go to if condition;
 Stop();
 }

❖ Detection using threshold setting

DetectionThr_value()

{

- Collect the parameter of an intruder which is consisting in ITable.
- Set the Thr_value() for all these parameters like for IP address set the value of DNS and response time (like 10ms).
- In config file fix the syntax of file, file name and in file system fix the value of APIs.

}

DetectionThr_valueAccess() // If an intruder attack into the system then Thr_value() detect the attack.

{

If (Intruder match with the fixed Thr_value()) // Fix low priority
 Detect an Intruder;
 Else
 Fix the Thr_value()=high; //Fix High priority
 }
 Go to if condition;
 End();
 }

Architecture of Intruder Detection

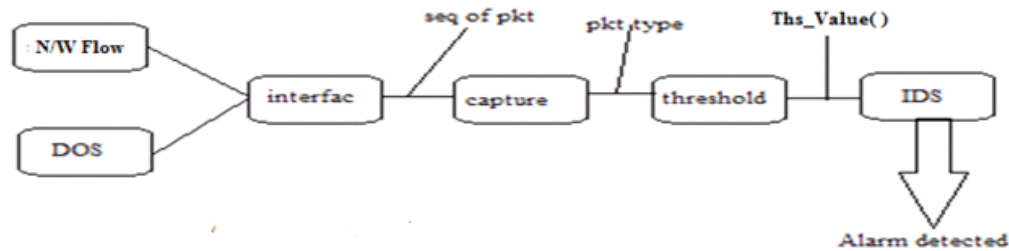


Figure 3.3: Architecture of Intruder Detection

In above Architecture of Intruder Detection represents the detection over the network. In this use the threshold value to detect the unauthorized access into network. In this capture the packets and compare with the threshold value and detect the alarm.

4. CONCLUSION

The proposed architecture and mechanism for taxonomy based intrusion attack and detection management scheme in Peer-to-Peer network is based on host system and network system. The knowledge and behavior system are used to better detection and provides better information about an intruder. Here provides an overview of the current state-of-the-art of intruder and its detection, based on a proposed taxonomy. This taxonomy highlights the properties of intrusion-detection systems and covers the past and current developments adequately. In this paper provides the detection mechanism for detect the intruder.

5. FUTURE SCOPE

The proposed architecture and mechanism for taxonomy based intrusion attack and detection management scheme in Peer-to-Peer network is effective, efficient and secure way of detecting the taxonomy based attacks but the detection provides the limited attack over the networks. Still remaining the progress with new approaches to both knowledge-based and behaviour-based intrusion detection or host and network based. The detection of abuse-of-privilege attacks is also the issues of current work.

6. Reference

- [1] Kavita Choudhary, Meenakshi, Shilpa, "Smurf Attacks: Attacks using ICMP", IJCST Vol. 2, Iss ue 1, March 2011, ISSN:2229-4333(Print)|ISSN:0976-8491(Online).
- [2] C.E.Landwehr et al., "A Taxonomy of Computer Program Security Flaws," ACM Comp. Surveys, vol. 26, no. 3, pp. 211-54, Sept. 1994.
- [3] Vinay M. igure, and Ronald d. williams, "taxonomies of attacks and vulnerabilities in computer systems", IEEE communications surveys, volume 10, no. 1, 1st quarter 2008.
- [4] K. Jiwnani and M. Zelkowitz, "Susceptibility Matrix: A New Aid to Software Auditing," IEEE Sec. & Privacy, vol. 2, no. 2, pp.16-21, Mar-Apr 2004.
- [5] D.G. Andersen. Mayday: Distributed filtering for internet services. In Proceedings of 4th Usenix Symposium on Internet Technologies and Systems, March 2003.
- [6] J.D.Howard and T.A.Longstaff, "A Common Language for Computer Security Incidents," Sandia tech. rep. SAND98-8667, Oct. 1998.

- [7] U.Lindquist and E. Jonsson, "How to Systematically Classify Computer Security intrusions," Proc. IEEE Symp. Sec. and Privacy, pp.154–634–7 May 1997.
- [8] J.Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Comp. Commun. Rev., vol. 34, no., pp. 39–53 2, Apr. 2004.
- [9] E. Fisch. A Taxonomy and implementation of automated responses to intrusive behavior. PhD thesis, Texas A&M University, 1996.
- [10] B.B.Gupta, R.C.Joshi, ManojMisra, "Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010.
- [11] Allen, W.H., Marin, G.A. & Rivera, L.A. (2005), "Automated detection of malicious reconnaissance to enhance network security", Proceedings IEEE, SoutheastCon, 2005.
- [12] A.K.Vatsa, Rizwan Khan, "Detection and Control of DDOS Attacks over Reputation and Score Based MANET", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 11, ISSN 2079-8407, October 2011.
- [13] V.Raskin, "Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool," Proc. New Sec. Paradigms Wksp., Cloudcroft, pp. 53–59, NM, 2001.
- [14] M.Bishop, "Vulnerabilities Analysis," Proc. 2nd Int'l. Symp. Recent Advances in Intrusion Detection, pp. 125–36, Sept. 1999.
- [15] D.L.Lough, "A Taxonomy of Computer Attacks with Applications to Wireless Networks," Ph.D. dissertation, Virginia Tech, Apr. 2001.
- [16] P.Rajapandian Dr.K.Alagarsamy, "Intrusion Detection in Dos Attacks" International Journal of Computer Applications (0975 – 8887), Volume 15– No.8, February 2011.
- [17] Zhongqiang Chen, Yuan Zhang, Zhongrong Chen and Alex Delis, "A Digest and Pattern Matching-Based Intrusion Detection Engine", The Computer Journal Advance Access published April 15, 2009.
- [18] Sandeep A. Thorat, Amit K. Khandelwal, Bezawada Bruhadeshwar and K. Kishore, "Anomalous Packet Detection using Partitioned Payload", Journal of Information Assurance and Security 3, 195-202, year 2008.
- [19] Revathi Cherukuri, Thadoor Shobha Rani, Challa Madhavi, Dr.Manjunath Gadiparthi, "A Real Time DOS Attack Detection in IP Networks Based on Bandwidth Utilization Pattern and Rule Based Pattern Matching", IJCST Vol. 2, Issue 3, , ISSN: 2229 - 4333 (Print) | ISSN : 0 9 7 6 - 8 4 91 (Online), September 2011.
- [20] Ketki Arora, Krishan Kumar, Monika Sachdeva, "Impact Analysis of Recent DDoS Attacks", Ketki Arora / International Journal on Computer Science and Engineering (IJCSE). Vol. 3 No. 877, ISSN: 0975-3397, 2 Feb 2011.
- [21] P.G.Neumann., "A Provably Secure Operating System," Tech. rep. SRI Project 2581, Contract DAAB03-73-C-1454, Prepared for USAECOM, Stanford Research Inst., 13 June, 1975.
- [22] P.G.Neumann, "Computer System Security Evaluation," Proc. Nat'l. Comp. Conf., vol. 47, pp. 1087–95., June 1978.
- [23] P.G.Neumann and D.B.Parker, "A Summary of Computer Misuse Techniques," Proc. 12th Nat'l Comp. Sec. Conf., pp. 396–407, 1989.
- [24] P.G.Neumann, Computer Related Risks, ACM Press, 1995.
- [25] S. Hansman and R. Hunt, "A Taxonomy of Network and Computer Attacks," Comp. & Sec., vol. 24, no. 1, pp. 31–43, Feb. 2005.
- [26] Stefan Axelsson, "Intrusion Detection Systems: A Survey and Taxonomy", 14 March 2000.
- [27] Vimal Upadhyay , Rajeev kumar, "Detecting And Preventing IP Spoofed Attack By Hashed Encryption" International Journal of Enterprise Computing and Business Systems, Vol. 1, Issue 2, July 2011.

- [28] Asmaa Shaker Ashoor , Prof. Sharad Gore, “How can distinguish between Hackers and Intruders”, 2011 International Conference on Future Information Technology, IPCSIT vol.13 (2011) © (2011) IACSIT Press, Singapore .
- [29] T.Toth. Improving Intrusion Detection Systems. PhD thesis, Technical University of Vienna, 2003.
- [30] T.Toth and C.Kruegel. “Evaluating the impact of automated intrusion response mechanisms”, In ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference, 2002.
- [31] Nirbhay Ahlawat and Chetan Sharma, “Classification And Prevention Of Distributed Denial Of Service Attacks”, Nirbhay Ahlawat Et Al. / (Ijaest) International Journal Of Advanced Engineering Sciences And Technologies Vol No. 3, Issue No. 1, 052 – 060.
- [32] C.J.Tucker, S.M.Furnell, B.V.Ghita and P.J.Brooke, “A new taxonomy for intrusion detection”.
- [33] Cheng Jin, chengjin, Kang G. Shin, “Hop-Count Filtering: An Effective Defense against Spoofed DDoS Traffic”, CCS'03, October 27–30, 2003, Washington, DC, USA.
- [34] P.Syverson, “A Taxonomy of Replay Attacks [cryptographic protocols],” Proc. Comp. Sec. Foundations Wksp., pp. 187–91, 14–16 June 1994.
- [35] N.Arumugam, C.Venkatesh, “A Trivial Scheme for Detecting and Preventing Fake IP Access of Network Server Using IPHP Filter”, European Journal of Scientific Research, Vol.53 No.2, pp.258-268 (2011).
- [36] Sandeep A.Thorat, Amit K.Khandelwal, Bezawada Bruhadeshwarand K.Kishore, “Anomalous Packet Detection using PartitionedPayload”, Journal of Information Assurance and Security”3 (2008) 195-202. Received August 20, 2008. 1554-1010 \$03.50 © Dynamic Publishers, Inc.
- [37] P.Syverson, “A Taxonomy of Replay Attacks [cryptographic protocols],” Proc. Comp. Sec. Foundations Wksp., pp. 187–91, 14–16 June 1994.
- [38] Herve´ Debar, Marc Dacier , Andreas Wespi, “Towards a taxonomy of intrusion-detection systems”, Computer Networks 805–822, 31 _1999.
- [39] W.Lee, W.Fan, M.Millerand, S.Stolfo, and E.Zadok, “Toward cost-sensitive modeling for intrusion detection and response”, in Journal of Computer Security, volume 10, 2000.
- [40] Natalia Stakhanova, Samik Basu and Johnny Wong, “A taxonomy of intrusion response systems”, Int. J. Information and Computer Security, Vol. 1, No. 1/2, 169, 2007.
- [41] S.M.Furnell, G.B.Magklaras and M.Papadaki, “A generic taxonomy for intrusion specification and response”.
- [43] J.Cannady, J.Harrell, “A comparative analysis of current intrusion detection technologies”, Proc. 4th Technology for Information Security Conf. (TISC'96), Houston, TX, May 1996.
- [44] T.Garvey, T.Lunt, “Model-based intrusion detection”, Proc. 14th National Computer Security Conf., pp. 372–385, October 1991.
- [45] D.Raghu, M.Arani, Ch. Raja Jacob, “Comparison of DDOS Attacks and Fast ICA Algorithms on The Basis of Time Complexity”, International Journal of Computer Applications in Engineering Sciences, ISSN: 2231-4946.
- [46] Harmeeet Kaur, Jasveer Singh, “Prevention of DDoS Attacks”, IJCST Vol. 2, Issue 4, Oct.-Dec.2011 ISSN: 0976-8491(Online)| ISSN:2229-4333(Print).

Authors

Prashant Kumar Singh is pursuing M-Tech in Computer Engineering from Shobhit University, Meerut. He obtained B.Tech degree in Information Technology from Shobhit Institute of Engineering & Technology, Meerut in 2009. He has been in teaching since last three years. Currently he is working as Lecturer in DVSJET, Meerut. His research interests are in MANET (Mobile Ad-Hoc network) and Network Security.



Avimanyou Kumar Vatsa is working as Assistant Professor and Coordinator - CSE at Shobhit University, Meerut, (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech(I.T.) from V.B.S. Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has been supervised several dissertation of M.Tech. students. He is on the editorial board and reviewers of several international and national journals in networks and security field. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).

