Effective and Reliable Countermeasures for Detecting DDOS Attack in IDS

Mohammad Abrahim Wani
Research Scholar
MMICT&BM
Maharishi Markendeshwar University.
Mullana Ambala Haryana

Rshma Chawla
Assistant Professor
MMICT&BM
Maharishi Markendeshwar University.
Mullana Ambala Haryana

***Abstract*--The most important communication channel now-a- days is the web technology, but this communication channel is threaten by set of actions called intrusions and complicated network based attacks such as denial of service and distributed denial of service attacks. Intrusions are set of actions by which the computing system is taken from secured state to compromised state. Distributed denial of service is an attack by which the legitimated users are victimized for service and resource available. Many research efforts have been proposed to fix these types of attacks, but no optimal solution has been addressed till date. In order to fix this gap a frame work is designed that handles all aspects of DoS/DDoS attacks in IDS. The proposed system has four major components: The information is processed by the controller that is collected from the Mobile Agents and on the detection of DDoS attack takes an appropriate action. The agent based mechanism is used to keep track of all the node details (e.g. bandwidth, node capacity, etc). The filtration unit filters the all incoming traffic and if any denial is detected the data is blocked temporarily and updates the buffer for future record. The filtered IPs are passed to enhanced filter unit where the client has to solve the puzzle for authentication, the puzzle problem uses the resources of illegitimate clients and increase the reliability of the system.**

Keywords: - Denial of service (DOS), Distributed Denial of Service (DDOS), Intrusion Detection System (IDS), Agents, Puzzle System

I. INTRODUCTION

Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks are used to spoil the access of shared resources from authentic users. In general, DOS/DDOS attacks block legitimate clients on the internet from having access to genuine services such as web sites. For instance, the valid users are denied for its services through attackers with several server requests. The CERT Coordinator centre website presents a complete list of resources which can be depleted by a DOS/DDOS attack [9]. The DOS/DDOS attacks are known from since 1980's; they have recently known widely to the general public. In October 2002, the Internet Root servers, the Domain Name servers (DNS), were victims of DDOS attack [17]. In August 2003, Microsoft's main website suffered from two DDOS attacks [36]. Preventing these attacks has become very important because the list of DDOS attack victims can extend up to thousand pages.

Denial of Service (DOS) attack is generated by a single machine (called attacker) to make a server or network unavailable to its legitimate users. DOS attack collapse or degrade the quality of service in unexpected manner because it consists of highly damageable attacks [11].

Distributed Denial of Service (DDOS) attack is an effort to flood a victim by means of network/machines through a volume of traffic that is generated by several machines. So to trace the IP source of attack and block these attacks is a tough task because machines are combined from several networks [12, 13]. DDOS attack uses a large number of hosts called zombie that are established from unauthenticated computers. These hosts namely zombie or bots are joined with each other to build a network called Botnet, which has an authority from the attacker to launch the DDOS attack [23].

Countermeasures to DOS attacks have been considered for years. Unluckily, many offered defense techniques are inactive in environment: it is the solitary task of the protector to detect and sort denials-of-service, while the attacker is secure from any punishment for decadent server resources. Such a defense mechanism is insufficient to defend in opposition to vast zombie capabilities to crush the victim. At the same time, it offers small incentive to the owners of Internet hosts to defend their computers from without knowing joining the zombie fleet given the minor interference of the DDoS tools on the compromised machines that host them [10] on the one hand and the major administrative overhead of malware defense on the other [15,16]. Paper proposes a multi-layer DDOS defense mechanism built upon two filters, one simple filter and another enhanced filter. The enhanced filter uses puzzle technique. Both approaches help to control attack flows, and support incremental deployment.

This paper is structured as follows: Section 2 describes the related literature. Section 3 and 4 justifies the concept of Intrusion Detection System and DDoS respectively. Section 5 explains the overview of Agents. Section 6 explains Existing Frame work of DDoS using Multi Agents. Section 7

Proposes an Efficient and Reliable Counter Measure for detecting DDoS attack in IDS. Section 8 explains the working Algorithm of proposed system and finally section 9 concludes with conclusion and future scope.

II. RELATED WORK

This section presents the related works & explores various challenges in the Intrusion Detection System. Many countermeasures have been designed to counterattack DDoS attacks but all of them consume resources of the IDS of the response system.

The concept of intrusion detection system starts in 1980 with the James Anderson (1980), which discusses the concept of monitoring the data over the local network by using some predefined profiles. With this the concept of intrusion and audit data came into lime light [8]. This beautiful concept made lot of improvement in auditing subsystems, and logically laid the base for formulation and development of intrusion detection systems [7]. The concept describes the basic design for audit trails, which was very much useful in understanding the performance of users. This concept makes an impressive impact on the world of security systems.

Author [29] in 1996 describes the overview of intrusion detection concepts and taxonomy was given. It introduces and discusses several commercial and public-domain IDS's available. The author also describes recent developments in conventional intrusion detection: Distributed, modular system which includes both anomaly and misuse detection. A peek at the new breed of pro-active, preventative tools so-called Delphic tools identifies the threats and risks in the very early attack stages.

Author [1] explains many machine learning techniques and various other methods to detect intrusions and have circulated those problems and scope for the future use.

Various Genetic Algorithms (GAs) and Genetic Programming (GP) have been used for recognizing intrusions in various situations. Several use Genetic Algorithms to achieve taxonomy regulations [29]. Genetic algorithms choose obligatory skills and chooses mainly admirable and slightest bound of various main functions in which unique Artificial Intelligence methods were used to design acquisition rules [30].

Author [32] proposed architecture to Intrusion Detection System based on neural networks and genetic algorithms, this architecture detects novel attacks , minimizes the false positive rate, and the problems of base rate fallacy was addressed.

The use of GAs for intrusion detection came into the consideration in 1995, when the authors [33] implemented several agent technology and GP to identify network anomalies [41]. For agents the use of GP used to resolve anomalous network behaviors and every agent can observe one constraint of the network audit data. The expected method has the advantage, that various small autonomous agents are used but it has difficulty in communicating between the agents and also if the agents are not appropriately initialized the training process can be time consuming.

Author [2, 40] described a method using GA to detect anomalous network intrusion. The approach includes both quantitative and categorical features of network data for deriving classification policy. However, the enclosure of quantitative feature can enhance detection rate but no investigational results are available.

Meadows [27], Aura et al. [5] and Dean and Stubblefield [17] explored an attack in which a great quantity of messages with fake signatures to reduce an authentication server's CPU cycles.

Lau et. al. in 2000 [23] has projected to apply queering algorithm in network routers to avoid DDoS attacks. This work planned solution for DDoS attacks as a whole and does not spotlight on a definite type of attack.

Cabrera et al. (2001) in [13] proposed solution that intended to shield web servers from attacks or to reduce its effect. Their resolution spreads over the organization's entire internet infrastructure.

Hussain et. al (2003) in [18] has proposed outline for classifying DoS attacks based on header contents, transient ramp-up behavior and spectral analysis.

Specht (2004) in [36] has projected taxonomies of Distributed Denial-of Service attacks, tools, and countermeasure to help decrease the possibility of DDoS problem and to smooth the progress of comprehensive solutions

Lee in 2004 described the DDOS attack and proposes taxonomies to illustrate the scale of DDOS attack, the characteristics of software attack tools used and the countermeasures available, but emphasized on the require of more inclusive solutions and respond to actions to DDOS attacks.

Seufert et. al (2007) in [37] has proposed a outline for data collection and traffic filtering. This comes close to detects attack from the source usage of the system. However expansion of this solution to use various algorithms is left for future.

Juneja et.al (2009) in [20] has proposed a multi agent framework for detecting, protecting and source tracing of DDoS attacks. This work projected solution for tracing DDoS attack but still number of agents required to get best possible results is not clear and desires to be tested.

Aarti Singh et.al (2010) [4] initiated with an argument of UDP attacks and it was set up that protective measure for the same is the need. This work projected an agent-based framework for preventing and detecting UDP flood attacks. Agent technology has proved to be hopeful and being demoralized in many other research areas. Thus projected framework seems to be capable although its performance and authentication in real life atmosphere is left as outlook work

Mohammed A. Saleh and Azizah Abdul Manaf (2014) [26] proposed and designed an substitute resolution called a flexible, collaborative, multilayer, DDoS prevention framework (FCMDPF), which handles all aspects of HTTP-based DoS/DDoS attacks. In distinction, it suffers from low rate of false negatives, since it was not capable to perceive and avoid all of flash crowd (FC) attacks. As well, it failed to validate and trace back some of incoming requests.

Jingtang Luo, Xiaolong Yang, (2014) [19] described a model that takes into account the understandable behaviors of TCP's congestion window adaptation mechanism; it can broadly evaluate attack effect from both attack pattern and network environment. The simulation results specify that the relative error of model remains around 10% for most attack patterns and network environments One of the consequences is that many presented defense strategies, particularly the ones that were designed and validated on the basis of inaccurate conclusions, maybe in actuality incapable to guard against shrew attack effectively.

III. INTRUSION DETECTION SYSTEM OVERVIEW

Intrusion Detection system is a software application that monitors system and network activities & reports the suspected intrusions as defined by the enable IDS policies. Some IDS reports the intrusion and some attempt to stop an intrusion attempt .An IDS works by examining and collecting information for unknown occurrences.

Intrusion detection system is divided into two parts. They are

- **Host based Ids:** Host Ids get audit data from host audit trails and detects attack against a single host.[2]
- **Network based Ids:** Use network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services and Detect attacks from network. [2]

Based on the types of network attacks available the network has to secure from these types of attacks. Different approaches are available to defend the network/system, Intrusion detection system is the one approach that is used for securing the system, and is considered as the first defense line in protecting the system/network, IDS is designed for monitoring and securing the system against the intrusions. An intrusion detection system in general is categorized on the three operable components [34]. The operable components are shown in figure.1

Data source is divided into the four different types which are generally called as: Host-based monitors, Network-based monitors, Application-based monitors and Target-based monitors.

The second module of an intrusion detection system is recognized as the analysis engine. This module collects the information from the data source and monitors the data for the possibility of attacks or other method of violations. The approaches used by the analysis engine can use one or both of the following analysis method [25]:

- Misuse/Signature-based detection
- Anomaly/Statistical detection

The third module of an intrusion detection system is the response manager. In simple form, the response manager resolves the inaccuracies (feasible intrusion attacks) only when they are found on the system, in the form of a response by informing someone or something [21].

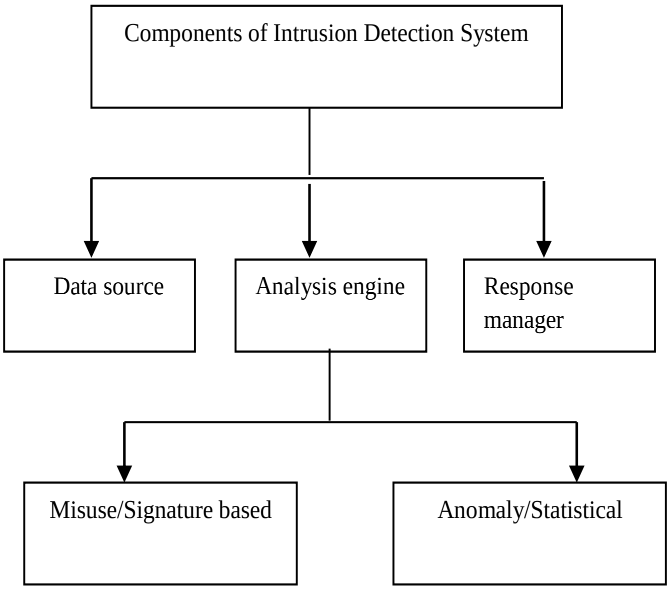

Fig. 1: Components of Intrusion Detection System

An IDS works by examining following events: observing activity, viruses, vulnerabilities, file settings, services, packet sniffing, PC check. The following show how IDS works;

- When the service stack detects forbid intrusion, it sends a message "an event" to IDS task.
- The IDS task's purpose is to counterpart each event in the (one at a time) line with normal form in port table. It also keeps a way and record of intrusive events.
- If any event exceeds a definite threshold according to IDS policies it generates a signal.
- If an event is signaled, the intrusion monitor authentication is formed in audit journal.
- The GUI of the Ids displays the intrusion events from the intrusion checking audit records.
- The system for message notification on IDS properties page, IDS notification sends an e-mail to particular email address.

IV. DDOS OVERVIEW

A Denial of service attack is a type of attack in which the hacker makes a computing or memory resources too busy or too full to provide justifiable networking requests and hence denying users access to a machine. The goal of a DoS attack is to disrupt some legitimate activity, such as browsing Web pages, listening to an online radio, transferring money from bank account, or even docking ships communicating with a naval port. This denial-of-service effect is achieved by sending messages to the target that interfere with its operation, and make it hang, crash, reboot, or do useless work.

There are many types of attacks crafted specially for [24]

- Congesting network resources.
- Draining CPU memory.
- Reducing computing power, Exploiting timers.
- Poisoning domain name translations etc.

There are many attacks that could be carried out at application level, hindering the normal functioning of a service. There are attacks that are designed to crash a web browser, email application or even a media player. When a specific application is disrupted and when normal functioning is hindered, it is called the Application level Denial of Service.

As a worst case scenario, there are attacks that can cause permanent damage to a system. These kinds of attacks are called the Permanent Denial of Service or Phlashing [40]. Permanent Denial of Service attacks are mostly firmware based that aims at completely destroying the hardware. Firmware's are the inbuilt code or program that is embedded on every electronic system for its proper functioning. When an attacker is able to change the firmware and replace it with a defective or corrupt one, the hardware could no longer be used. These attacks could be directed towards networking components like routers, switches or bridges and thus bringing an entire routing table to collapse. A fault in a single router might lead to a huge outage if it does not have enough backups and rerouting. Some devices, who try to upgrade their firmware online without checking for the signature of a trusted source, fall prey for this attack.

A. Various methods used for DDoS attack

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

A DoS attack can be perpetrated in a number of ways. Attacks can fundamentally be classified into five families [31]:

1. Consumption of computational resources, such as bandwidth, memory, disk space, or processor time.
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack may include execution of malware intended to [31]:

- Max out the processors usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to

Use up all available facilities so no real work can be accomplished or it can crash the system/operating system itself [24].

In most cases DoS attacks involve forging of IP sender addresses (IP address spoofing) so that the location of the attacking machines cannot easily be identified and to prevent filtering of the packets based on the source address.

Denial of Service attack is generally carried out with large number of systems attacking a specific victim. Such an attacking network is called the Botnet. A Botnet is formed by thousands of slave systems usually termed as the Zombies. The attacking systems are often controlled and manipulated by a remote attacker who makes use of these compromised machines. Most of the times, the real owner of a compromised machine is not aware of the malicious activities. Next section represents the use of Agent technologies in monitoring DDoS attacks.

V. AGENTS OVERVIEW

An agent is a software entity or a mixture of hardware or software entity which has the capability to perform on behalf of its users in parallel. It is possessed with many helpful features like cooperation, learning ability, reactivity and pro-activity.

The software agents not only offer the competitive lead by improving process feature but also combine the new technology and specialized expertise. Agent technology finds its applications in broad areas such as user interfaces, mobile computing, information retrieval and filtering, smart messaging, telecommunications and the electronic marketplace. The smart agents work together with each other in a multi-agent system in different ways. The clusters of agents in a multi-agent framework are competitive, cooperative, and task-oriented and can also provide an interface to users. The characteristics that motivated the use of software agents in DDoS attacks are their security monitoring capabilities like: autonomy, fault tolerance, robust, dynamic-configuration, information providers, task oriented and scalable [20]. Possessed with all such capabilities, agents can positively be functional in avoidance of DDoS attacks.

VI. EXISTING FRAMEWORK

The attacks of DDoS fundamentally consume the computational resources, memory etc. So researchers are using the methods to counterattack these attacks with different techniques and the existing framework is designed which is based on the agents that capable the source tracing of detecting any attack. The framework consists of agents including Mobile Agent (MA), Filter (F), Host Agent (HA), and Controller (C). The pictorial representation of the Framework is shown in figure 2. Due to the movement from private internet to public internet, organizations have flat hackers that disturb the private data, so securing the private data becomes the great and big issue in front of the holder. This work proposed a framework that detect, prevent and traces the sources of the attack. The framework has a capability of tracing a source apart of detecting any attack.

This work projected solution for tracing DDoS attack but still number of agents required to get best possible results is not clear and desires to be tested. The overall system performance can be increased with the advancement in architecture, and the bandwidth of the system can be increased if the illegitimate users will be busy with their own resource.

The proposed framework is architected in keeping these points in view so that the illegitimate user can be avoided as long as possible.

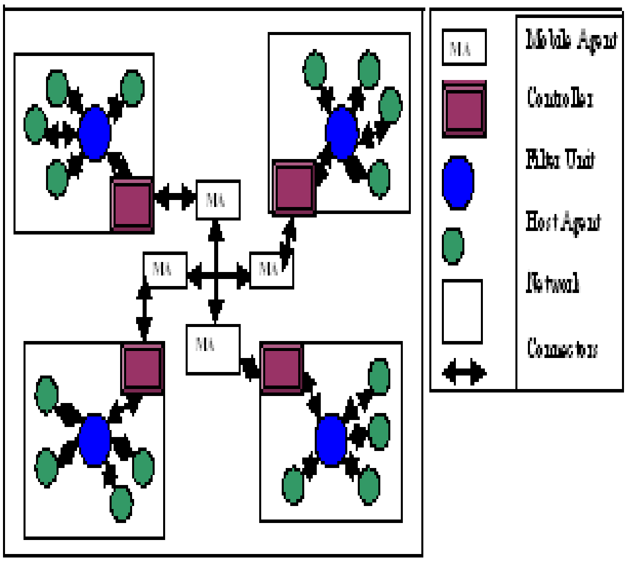

Fig. 2: The Existing Framework [20]

VII. PROPOSED FRAMEWORK

This section proposes a framework that detects and aims to identify, avoid & achieve source tracing of DDOS attack at a network site. The framework uses both the approaches of IDS (i.e. Anomaly based and Signature based) to increase the reliability of the system. The resource utilization of the previous framework is reduced by dinning the traffic of illegitimate users by the approach of puzzle system. A pictorial representation of the framework is given in a figure 3. The proposed frame work comprises of 5 components namely Mobile Agents (MA), Host Agents (HA), Controller(C), Filter (F) and Enhanced Filter (EF).

Mobile Agents: - Mobile Agents (MA) provides communication from source to destination. Each agent gathers information from and within a network of hosts and forward to collectors at the destination end. Mobile agents are attached with a history buffer which is updated to maintain record.

Host Agents: - Host agents collect information provided by filters. Filter provides filtered information to Enhanced filter unit.

Controller: - The information is processed by controller that is collected from Mobile Agents, and if any DDOS attack is detected by filter it takes appropriate action. It also checks the compromised state of machines if found then it locates the master and communicate with the networks, therefore doing source tracing.

Filter: - The criteria of DDOS attack check is hold by Filter unit, it also contains history buffer to maintain the record of blocked IPS and update it periodically.

Enhanced Filter: - Enhanced Filter takes the valid IPS from filter unit and does the filtration at enhanced level and passes the valid data to host agents.

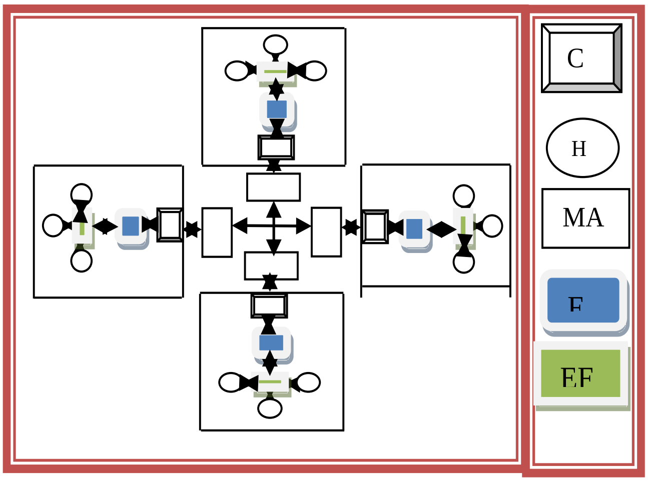

Fig. 3: The proposed Framework

The flow chart of the proposed framework is given the next section.

VIII. FLOW CHART OF PROPOSED FRAMEWORK

MA obtains information not only from its adjacent MAs but also from controller engaged at source. The controller collects this information and passes to the filter, filter verifies source and destination IPs and employs threshold, signatures, doubtful source and IDs to check that whether it is a DDOS, if check is true it alerts the controller and blocks all incoming traffic for a certain period of time. The alert message is forwarded to all connected MAs through controller which is responsible to trace the source attack. The HOP method is used to check the source attack one by one until the compromised HOP is traced.

When the incoming traffic is accepted a valid source by filter, incoming traffic is passed to enhanced filter where the client has to solve the puzzle to validate its identity. The enhanced filter uses web service technology to create a puzzle, random number and nonce value and goes back to client or requester for puzzle solution. The requester has to solve the puzzle by means of a random number (web applications), after solving puzzle, the client sends back the puzzle's answer, along with the nonce value. After that, the web server (web application) will validate puzzle's answer and nonce value that are sent by the client whether they are correct or not. If both numbers are correct, the request will be forwarded to the host agent. Otherwise it will be blocked immediately and a signal is sent back to the edge router to update its black list.

Goal of puzzle problem One of the main goals of puzzle problem is to reduce the load on the server, thus, allowing it to handle more connections and improve overall system performance. The strength of puzzle problem to defeat a DDOS attack is based on the fact that that the attacker will be asked for solving one puzzle for each service request and solving all the puzzles will exhaust the attacker's resources, and hence the overall performance of the legitimate users will increase.

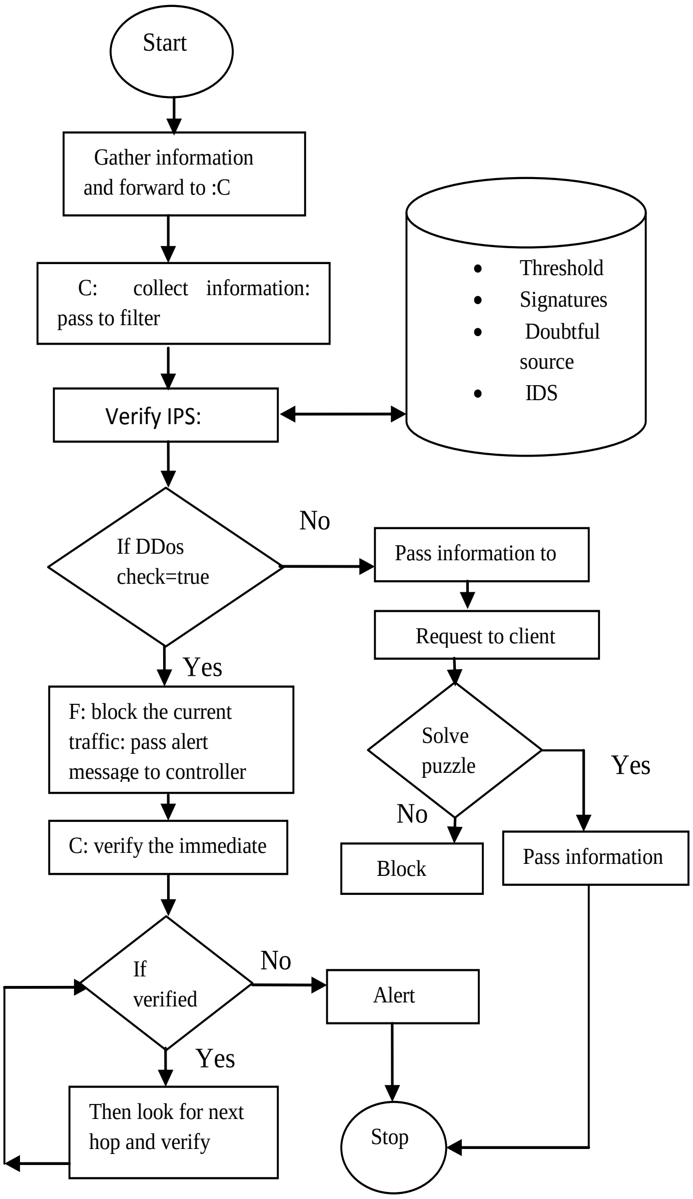

Fig. 4: Flow chart of Proposed Framework

IX. CONCLUSION AND FUTURE SCOPE

In the current scenario, the Denial of Services is dangerous for the smooth functioning of network. The active defense mechanism fades away from these threats by which the cost for delivering attack traffic raises. In this paper we describe our framework for DDoS defense technique based on two filters, one the simple filter and another enhanced filter. It is not constantly feasible to completely avoid attacks because there will for eternity be susceptible hosts in the internet to be compromised for attack purposes and also many DDoS attack mechanisms are available. But the projected technique of detecting and avoiding attacks will be more efficient and effective than the existing methods showing an enhanced performance.

REFERENCES

1. Anjali Karar, "Intrusion detection and fighting with Intrusions: a survey", International Journal of Computer Science & Information Technology, Vol. 3 No. 6 June 2013, pp.no 235-242
2. Rshma, "Detection of DDOS attacks using data mining", international journal of computing and business research, vol. 2, issue 1, 2011.
3. Bilal Maqbool, and M. A. Peer. "Intrusion Detection and Prevention System: Classification and Quick." (2011).
4. Aarti Singh et. al, "Agent Based Preventive Measure for UDP Flood Attack in DDoS Attacks", International Journal of Engineering Science and Technology Vol. 2(8), 2010, pp. 3405-34
5. Aura, Nikander, P. Leiwo, "Dos-resistant authentication with client puzzles", In Proceedings of the Cambridge Security Protocols Workshop 2000. LNCS. Springer, Heidelberg (2000)
6. AurobindoSundaram, "An introduction to intrusion detection systems" published in Magazine- special issues on computer security volume 2 issue 4, March 1996, pp 3-7
7. Chawla, "Software security pattern in security Engineering", IJRIM, vol. 2, issue 2, February 2012.
8. CERT Coordination Centre, "Denial of Service Attacks," Tech Tips, June 2001
9. CERT. Computer emergency response team, cert advisory ca-2001-01: Denial-of-service developments. 2000. http://staff.washington.edu/ dittrich/misc/ddos
10. C.Qi,W,Lin,W.Dou, and S.Yu, "CBF: a packet filtering method for DDoS attack Defense in cloud environment," in Proceedings of the 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11), Sydney, Australia, December 2011.
11. C.-T.Xia, X.-H.Du, L.-F.Cao, and H.-C.Chen, "An algorithm of detecting and defending CC attack in real time," in Proceedings of the International Conference on Industrial Control and Electronics Engineering (ICICEE '12), pp. 1804–1806,August 2012.
12. Chonka, W. Zhou, J. Singh, and Y. Xiang, "Detecting and tracing DDoS attacks by intelligent decision prototype," in Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 08), pp. 578–583, March 2008.
13. Cabrera J. B. D, Lewis L, Qin X., Lee W, Prasanth R.K., Ravichandran B. and Mehra R. K., "Proactive Detection of Distributed Denial of Service Attacks using MIB Traffic

Variables - A Feasibility Study", Proceedings of the 7th IFIP/IEEE International Symposium on Integrated Network Management, Seattle, WA - May 14-18, 2001.

14. Dietrich, S. Long, N. Dittrich, "Analyzing distributed denial of service attack tools: The shaft case", In: Proceedings of 14th Systems Administration Conference, LISA 2000
15. Dittrich D, "Distributed denial of service (DDoS) attacks/tools", resource page (2000) http:// staff .washington.edu/dittrich/misc/ddos
16. Duffy Marson C, and Gareston C, "Net Security Gets Root-Level Boost", Network World Fusion, October 2003
17. Dean D, Stubblefield A, "Using client puzzles to protect tls", In: Proceedings of 10th Annual USENIX Security Symposium (2001)
18. Hussain A, Heidemann J, and Papadopoulos C, "A Framework for Classifying Denial-of-Service Attacks", Karlsruhe, Germany, pp. 99–110, 2003.
19. Jing tang Lou, Xiao long Yang, "On a Mathematical Model for Low-Rate Shrew DDoS" IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, July 2014.pp.no 1063-1083
20. Juneja D, Chawla R, and Singh A, "An Agent-Based Framework to counter attack DDoS Attacks", International Journal of Wireless Networks and Communications, Vol. 1, No. 2, pp. 193 – 200, 2009.
21. J. McHugh, "Intrusion and intrusion detection", International Journal of Information Security (2001), no. 1, pp.no 14–35
22. L. Yang, T. Zhang, J. Song, J. Wang, and P. Chen, "Defense of DDoS attack for cloud computing", in Proceedings of the IEEE International Conference on Computer Science and Automation Engineering (CSAE 12), Zhangjiajie, China, pp. 626–629, May 2012.
23. Lau F, Rubin S, Smith M, and Trajkovie L, "Distributed Denial-of-Service Attack", In IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN USA, October 2000, pp. 2275-2280
24. LIU, "Surviving Distributed Denial-Of-Service Attacks," IEEE Computer, Vol. 11, no, 5, Sep. 2009, PP.no 51-53
25. Mohammad SazzadulHoque, Md. Abdul Mukit and Md. Abu NaserBikas, "An implementation of intrusion detection system using genetic algorithm" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012 p.no 111
26. Mohammed A. Saleh, and Azizah Abdul Manaf, "A Novel Protective Framework for Defeating HTTP-Based Denial of Service and Distributed Denial of Service Attacks", Hindawi Publishing Corporation. The Scientific World Journal 7 September 2014.
27. Meadows C, "A cost-based framework for analysis of denial of service networks", J. Computer. Secure. Vol. 9, pp. no 143–164 year 2001
28. M. Pillai, J. H. P. Eloff, H. S. Venter, "An Approach to Implement a Network Intrusion Detection System using Genetic Algorithms", Proceedings of SAICSIT, pp:221- 228, 2004.
29. M. Middlemiss, G. Dick, "Feature selection of intrusion detection data using a hybrid genetic algorithm/KNN approach", Design and application of hybrid intelligent systems, IOS Press Amsterdam, pp.519-527, 2003.
30. M. Crosbie, E. Spafford, "Applying Genetic Programming to Intrusion Detection", Proceedings of the AAAI Fall Symposium, 1995.
31. MeghnaChhabra, "A Novel Solution to Handle DDOS Attack in MANET", Journal of Information Security, Vol. 4 No. 3 (2013), Article ID: 34631, pp. no 165-179
32. Prasad, "An Intrusion Detection System Architecture Based on Neural Networks and Genetic Algorithms", International Journal of Computer Science and Management Research, Vol 2 Issue 1 January 2013, pp.no 1344-1361
33. R. H. Gong, M. Zulkernine, P. Abolmaesumi, "A Software Implementation of a Genetic Algorithm Based Approach to Network Intrusion Detection", 2005.
34. R. G. Bace, "Intrusion Detection", Macmillan Technical Publishing. 2000.
35. Stallings and William, "Cryptography and Network Security Principles and Practices", Upper Saddle River, NJ, Prentice Hall, 2003
36. Specht S, and Lee R, "Distributed Denial-of-Service: Taxonomies of Attacks, Tools and Countermeasures", Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, pp. 543-550, September 2004.
37. Seufert S, and O'Brien D, "Machine Learning for Automatic Defense against Distributed Denial- of-Service Attacks", International Conference on Communications (ICC'07), pp. 1217-1222, 24-28 June 2007
38. Rshma , 'Software development Effort estimation techniques: A review", international journal of eclectronics communication and computer engineering. Vol. 5, issue 5, September 2014.
39. Garg, "Study of network and transport layer protocols to exploit the potential of higher layers in mobility management", international journal if science and research, vol. 3, issue 11, November 2014
40. U. D. Khartad, and R. K. Krishna, "Route Request Flooding Attack Using Trust Based Security Scheme in Manet," International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), Vol. 1, No. 4, 2012, p. 27.
41. W. Li, "A Genetic Algorithm Approach to Network Intrusion Detection", SANS Institute, USA, 2004.