WWJMRD 2017; 3(11): 352-356
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Renuka Sharma
Student, MRSTU, Bathinda, Punjab India

Abhilasha Jain
Associate Professor, MRSTU, Bathinda, Punjab, India

Correspondence:
Renuka Sharma
Student, MRSTU, Bathinda, Punjab India

DDoS Detection using Hybrid technique of PSO and Fire Fly

Renuka Sharma, Abhilasha Jain

Abstract
Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. DDOS type of attack is the serious threat to the nodes in the internet. Various attackers lying in the distributed manner can attack the network so that there will be slow unnecessary requests to the server. Which in results overload the network. In existing research Packet Size based technique was used. In which delay Packet Size is calculated for the sample in time interval T. if the Packet Size value is greater than the threshold value then attacker is assumed. In current research hybrid approach based on PSO and Firefly is used. It identifies the optimal application server where the request can be sent. This optimality is checked based in delay it is producing. This approach has shown positive results. The performance parameters like end to end Delay, packet Delivery Ratio and Throughput has shown improvement. That means hybrid approach considered in current research has shown the improvements.

Keywords: Firefly, PSO, Wormhole Attacker

Introduction

Cyber Security

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Governments, military, corporations, financial institutions, hospitals and other businesses collect, process and store a great deal of confidential information on computers and transmit that data across networks to other computers. With the growing volume and sophistication of cyber-attacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. During a Senate hearing in March 2013, the nation's top intelligence officials warned that cyber-attacks and digital spying are the top threat to national security, eclipsing terrorism [2].
Cyber risks can be divided into three distinct areas:

- **Cyber crime**
  Conducted by individuals working alone, or in organised groups, intent on extracting money, data or causing disruption, cybercrime can take many forms, including the acquisition of credit/debit card data and intellectual property, and impairing the operations of a website or service.

- **Cyber war**
  A nation state conducting sabotage and espionage against another nation in order to cause disruption or to extract data. This could involve the use of Advanced Persistent Threats (APTs)

- **Cyber terror**
  An organization, working independently of a nation state, conducting terrorist activities through the medium of cyberspace. Organizations that have to consider measures against cyber war or cyber terror include governments, those within the critical national infrastructure, and very high-profile institutions. It is unlikely that most organizations will face the threat of cyber war or cyber terror.

Cyber criminals operate remotely, in what is called 'automation at a distance', using numerous means of attack available, which broadly fall under the umbrella term of malware (malicious software). These include:

- **Viruses**
  Aim: Gain access to, steal, modify and/or corrupt information and files from a targeted computer system.
  Technique: A small piece of software program that can replicate itself and spread from one computer to another by attaching itself to another computer file.

- **Worms**
  Aim: By exploiting weaknesses in operating systems, worms seek to damage networks and often deliver payloads which allow remote control of the infected computer.
  Technique: Worms are self-replicating and do not require a program to attach themselves to. Worms continually look for vulnerabilities and report back to the worm author when weaknesses are discovered.

- **Spyware/Adware [4]**
  Aim: To take control of your computer and/or to collect personal information without your knowledge.
  Technique: By opening attachments, clicking links or downloading infected software, spyware/adware is installed on your computer.

- **Trojans**
  Aim: To create a 'backdoor' on your computer by which information can be stolen and damage caused.
  Technique: A software program appears to perform one function (for example, virus removal) but actually acts as something else.

DDOS Attack

Denial of Service (DoS) is a class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine

There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Exploiting the system's misconfigurations.
- Targeting the implementations bugs.

DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users.

Types of DDOS attacks

Various types of DDoS attacks are given below:

a. Application Level Attacks
b. Degradation of Service Attacks
c. Multi-Vector Attacks
d. Nuke
e. Peer-to-Peer Attacks
f. Ping of Death
g. Reflected Attack
h. Slow Loris
i. SYN Flood
j. UDP Flood (User Datagram Protocol)
k. Unintentional DDoS
l. Zero Day DDoS

Particle Wsarm Optimization

Particle swarm optimization (PSO) is a population based stochastic optimization technique developed by Dr. Eberhart and Dr. Kennedy in 1995, inspired by social behavior of bird flocking or fish schooling.

PSO shares many similarities with evolutionary computation techniques such as Genetic Algorithms (GA). The system is initialized with a population of random solutions and searches for optima by updating generations. However, unlike GA, PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, fly through the problem space by following the current optimum particles.

Firefly Optimization Algorithm

Firefly Algorithm (FA) is a metaheuristic algorithm for global optimization, which is inspired by flashing behavior of firefly insects. This algorithm is proposed by Xin-She Yang in 2008. Fireflies use the flashing behavior to attract other fireflies, usually for sending signals to opposite sex. However, in the mathematical model, used inside Firefly Algorithm, simply the fireflies are unisex, and any firefly can attract other fireflies.

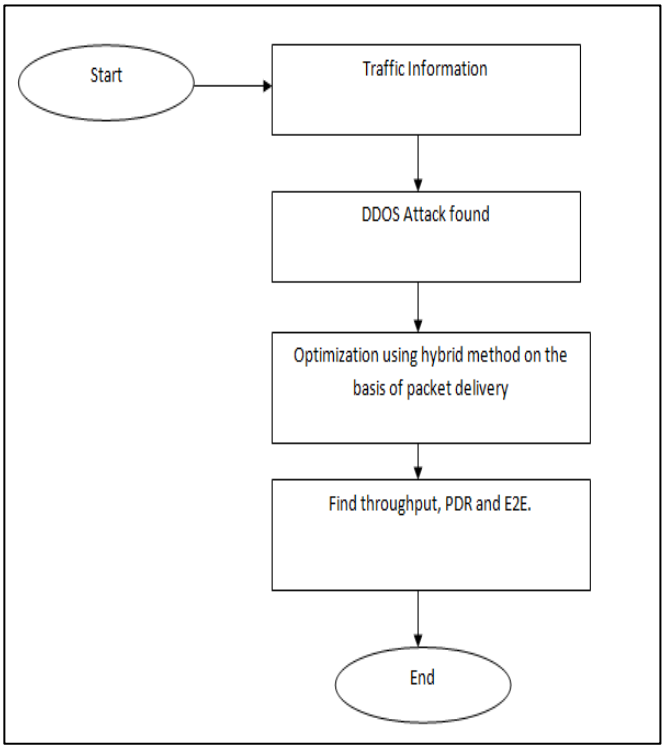
Literature Survey

Monowar H. Bhuyan et al. [9] Invasion by Distributed Denial of Service (DDoS) is a serious threat to services offered on the Internet. A low-rate DDoS attack allows legitimate network traffic to pass and consumes low bandwidth. So, detection of this type of attacks is very difficult in high speed networks. Information theory is popular because it allows quantifications of the difference between malicious traffic and legitimate traffic based on probability distributions. In this paper, we empirically evaluate several information metrics, namely, Hartley entropy, Shannon entropy, Renyi's entropy and generalized entropy in their ability to detect low-rate DDoS attacks. These metrics can be used to describe characteristics of network traffic and an appropriate metric facilitates building an effective model to detect low-rate DDoS attacks. We use MIT Lincoln Laboratory and CAIDA DDoS datasets to illustrate the efficiency and effectiveness of each metric for detecting mainly low-rate DDoS attacks.

1. **Xiao et al.** presented an approach that uses information theory and GA to detect abnormal network behaviours. Based on the mutual information between network features and the types of network intrusions, a small number of network features are closely identified with network attacks. Then a linear structure rule is derived using the selected features and a GA. The use of mutual information reduces the complexity of GA, and the single resulting linear rule makes intrusion detection efficient in real-time environment. However, the approach considers only discrete features.

2. **Li** presented an approach to detect network anomalous using Genetic Algorithm. The detection rates may be increased due to quantitative features inclusion. Parameters and evolution processes for GA are discussed in details and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus reduce the complexity. To implement and measure the performance of this system they used the KDD99 benchmark dataset and obtained reasonable detection rate.
3. **Bridges** implemented a method to detect both anomalies and network misuses by combing Genetic Algorithm‟s and Fuzzy data mining technologies. In this method select the most significant network features and locate the best possible parameters of the fuzzy function by using Genetic Algorithm.
4. **Crosbie** proposed a methodology to detect network anomalies using Genetic Programming (GP) and multiple agent technology. When the agents are not properly initialized, the training process takes long time. The communication among small autonomous agents is still a problem.
5. **Selvakani** Applied Genetic Algorithm to generate rules for training the IDS. Rules are generated for only Smurf (DoS) attack and Warzemaster (R2L) attack. This performance of this methodology detection rate is low. This survey shows that the proposed Intrusion Detection models for R2L, U2R, Probe attacks get low detection rates using KDDCup dataset. This paper studies two types of attacks for each category i.e., DoS, R2L, U2R and Probe. Observed all the features in the KDDCUP Dataset to detect the attacks.
6. **Lu** Develop a method to derive a set of classification rules by using Genetic Programming (GP) with help of past data of network. In this method using GP the practical implementation is more difficult due to the system required more data or time.

Flowchart



Algorithm

Step1 DDoS is not a single kind of network attack but a general name of different kinds of attack strategies that exploit the loopholes in existing security systems and protocols to disrupt the victim's resources.

Step2 Before launching the attack, an attacker sends ICMP Echo packets to find the machines which are vulnerable to security threat and gains their access. Once those machines are compromised, those become the agents to consolidate a DDoS attack towards a single destination.

Step3 Distribution of Source and Destination IP addresses and ports in existing network provide information about the DDoS attack.

Step4 During the attack period the destination IP address becomes common in each packet trace. The self-similarity of each network that exists regardless of network type, protocols, topology and packet size plays a crucial role in statistical anomaly detection. I

Step5 if the http request data is abnormally small it may be the reason of slow read packets. Http packet timeline is important to consider for mitigating slow http request attack.

Step6 Attacker machine requests with extremely slow packet transfer rate that keeps the server's resources always busy.

Step7 Then DDOS attack prevention will be done using PSO as well as Firefly method.

Results Analysis

Current research is based on identification of DDOS using hybrid approach of PSO and FIREFLY. In current approach they have used the entropy based technique. In this technique for sample in time interval T. If delay entropy is greater than the threshold delay of the network of protocol previous router will raise the alarm. It will stop the data forwarding. So that overload at the server is not taken place. In current hybrid approach first most appropriate servers will be identified using fire fly mechanism. And using PSO optimal router for data packet forwarding will be identified. This will enhance the performance.

Network Configuration

Table 1: Network Configuration

Parameter	Value
Network Size	1000*1000
Application servers	9
Clients	3
Attacker	1
Packet Size	512Bytes
Request Packet	128 Bytes
Speed of Transfer	512 Bps

Performance Parameter

- **Packet Delivery Ratio:** It is defined as the ratio of the no. of packages received at the destination-node and np is the no. of packages which are sent by the source node. Here, $pckd_u$ is the no. of packages which are received by the specific destination-node in the u^{th} application, and $pcks_u$ is the nos. of packages sent by the source-node in the u^{th} application. The average Packet Delivery Ratio of the application traffic n, which is denoted by PDR, is obtained as

$$PDR = \frac{1}{np}\sum_{u=1}^{np}\frac{pcktd_u}{pcks_u}$$

- **End-to-End Delay:** This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is dn_u, and the number of packets received by the destination node is $pckdn_u$. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as

$$E = \frac{1}{np}\sum_{u=1}^{np}\frac{dn_u}{pckdn_u}$$

- **Throughput:** This is defined as the total amount of data (td_u) that the destination receives them from the source divided by the time (t_u) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by T, is obtained as

$$T = \frac{1}{np}\sum_{u=1}^{np}\frac{td_u}{t_u}$$

Interface

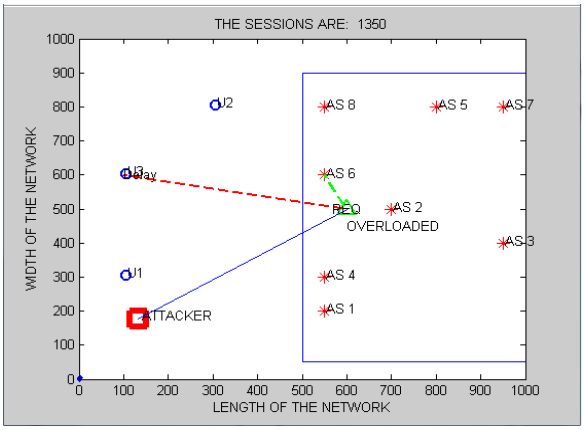


Fig. 1: Interface for Network

This interface is generated using MATLAB. In this interface we have taken 9 Application servers, one attacker and three clients. Each time attacker sends the request. Using DDOS it generates the overload at the application server level.

Packet Delivery Ratio

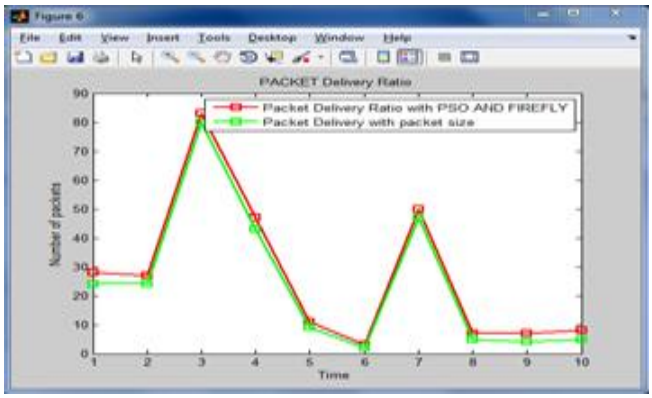


Fig. 2: Packet Delivery Ratio Comparison for With and Without DDOS

Graph shows that the packet delivery ratio in hybrid approach is improving compared to entropy based approach. In the middle of figure 4.2 for hybrid approach the packet delivery ration builds higher point. Shows packet delivery ratio has improved.

End to End Delay

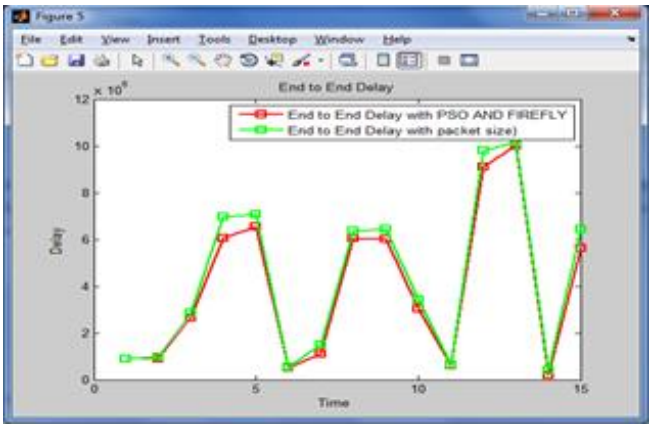


Fig. 3: End to End Delay Comparison for With and Without DDOS

In these graphs it is clear that the end to end delay has reduced in case of hybrid approach shown in figure 4.4. in hybrid approach the end to end delay builds large bottoms compared to the entropy based approach.

Throughput

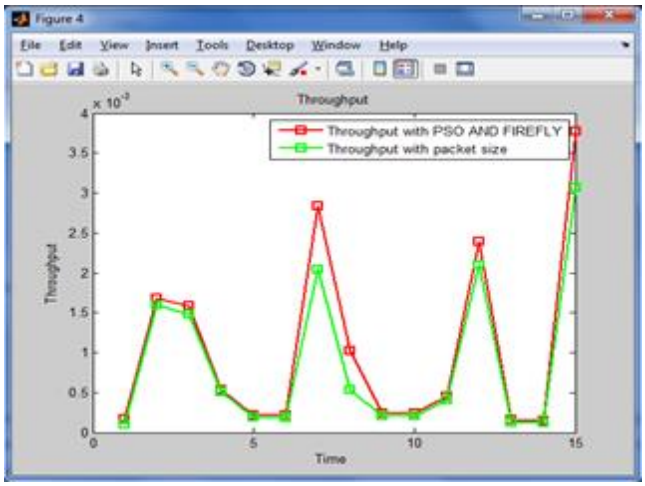


Fig. 4: Throughput Comparison for With and Without DDOS

Throughput for Hybrid approach has improved over to entropy based approach. In case of hybrid approach shown in fig. 4.6 build higher top. That means more packets are being delivered to the destination.

Percentage improvement

Table 2: Performance Comparison

Parameter	With Entropy	With PSO and Firefly	Improvement
Throughput	0.0020	0.091	97.71%
End to End Delay	1.05	0.43	55.99%
Packet Delivery Ratio	0.27	20.60	98.64%

Conclusion

DDOS type of attack is the serious threat to the nodes in the internet. Various attackers lying in the distributed manner can attack the network so that there will be slow unnecessary requests to the server. Which in results overload the network. In existing research Packet Size based technique was used. In which delay Packet Size is calculated for the sample in time interval T. if the Packet Size value is greater than the threshold value then attacker is assumed. In current research hybrid approach based on PSO and Firefly is used. It identifies the optimal application server where the request can be sent. This optimality is checked based in delay it is producing. This approach has shown positive results. The performance parameters like end to end Delay, packet Delivery Ratio and Throughput has shown improvement. That means hybrid approach considered in current research has shown the improvements. Current research is based hybrid approach of PSO and Firefly. This optimal approach has been taken over to the Packet Size based approach. In future this technique can be applied on other types of attacks.

References

1. T. Xiao, G. Qu, S. Hariri, and M. Yousif, “An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm”, Proceedings of the 24th IEEE International Performance Computing and Communications Conference (IPCCC „05), Phoenix, AZ, USA. 2005. Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Net, 2005.
2. W. Li, “Using Genetic Algorithm for Network Intrusion Detection”. “A Genetic Algorithm Approach to Network Intrusion Detection”. SANS Institute, USA, 2004.
3. Bridges, Susan, Rayford B. Vaughn,“ Intrusion Detection via Fuzzy Data Mining”, In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, Ottawa, Canada, 2000.
4. Crosbie, Mark, Gene Spafford, “Applying Genetic Programming to Intrusion Detection”, In Proceeding of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8, Cambridge, Massachusetts, 1995.
5. Selvakani S, R.S. Rajesh,” Genetic Algorithm for framing rules for Intrusion Detection”, IJCSNS, Vol.7, No.11, 2007.
6. W. Lu, I. Traore,“Detecting new forms of network intrusion using genetic programming”, Computational Intelligence Vol.20, Issue 3, pp. 475-494, 2004.
7. J. Cannady, "Artificial Neural Networks for Misuse Detection", In Proceedings of National Information Systems Security Conference, 1998.
8. B.C. Rhodes, J.A. Mahaffey, and J. D. Cannady, "Multiple Self-Organizing Maps for Intrusion Detection", In Proceedings of 23rd National Information Systems Security Conference, 2000.
9. Monowar H. Bhuyan, D. K. Bhattacharyya, J. K. Kalita,” Information Metrics for Low-rate DDoS Attack Detection : A Comparative Evaluation”, 2014