Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

DDOS Detection using Attack Model

Neha Titarmare, * Priyanka Gonnade, Punam Marbate
CSE Dept, RGCER, Nagpur,
India

Nayan Hargule
CE Dept, SCET, Nagpur,
India

Abstract— In today's world Distributed Denial of Service Attacks (DDoS) continue to pose a hazardous threat to cyber world. These attacks are still evolving and there is an utmost need to develop mechanisms which can be effective against them. It is however not easy to deal with such attacks. In this paper, we concentrate to develop attack model which gives us an idea about the patterns of the DDoS attacks. Our method maps flows of each attack pattern into an attack model. In this work we develop four types of attack models for the following DDoS attacks: Host scan, Port scan, TCP SYN flood, ICMP flood. Using these attack models we try to detect the above mentioned attacks by comparing the attack models with the incoming traffic.

Keywords—Attack model, DDoS, Host Scan, Port Scan

I. INTRODUCTION

DoS attacks are one of the crucial threats posed to the users and infrastructures of the Internet. A DoS attack attempts to deprive the legitimate users from using their service. It breakdowns the service and disrupt the network bandwidth. DoS attack can be launched from a single host or a network node. DDoS attacks pose a more serious threat than DoS attacks. DDoS is a type of DoS attack where an attacker deploys a number of hosts and launches an attack on the victim in a coordinated manner or simultaneously. The goal of DDoS attack is achieved by sending a large number of packets to the target and thus flooding it. The target is unable to deal with the large number of packets and gets overloaded, and ultimately becomes incapable of providing normal service. Well known DDoS flooding attacks are TCP SYN flood attack and ICMP flood attack. TCP SYN flood makes use of TCP SYN packets while ICMP flood makes use of ICMP packets. Before attacking the target, the attacker often uses host scan and port scan to check the services that they can break into. Host scan and port scan are used as tools to check the vulnerability of the target. If host scan and port scan is carried out frequently then it can be considered as an attack. Generally, host scanning and port scanning is done to keep a watch on the systems and the network. A network administrator usually performs these scans to check network and scanning is done a fixed number of time. However, if the number of scans surpasses a fixed threshold then they are considered as attack. In host scan attack, the attacker scans or
analyses the other host computer, so as to gain their information such as services available, and check their vulnerability. Port scan attack is performed to check the active ports and services provided by them. The objective of this is to find the vulnerable ports of a target host [2] [12].

In most of the previous work [5] [11] an attack model is described as a model where an attack is generated. In this paper, we propose an attack model to extract the attack patterns for the attack. These attack patterns help us to identify the type of attack, nature and its characteristics. The purpose of attack model is to effectively differentiate between attack flow and normal flow. Differentiating the attack flow facilitates effective detection of specific attacks. Our technique is based on the concept of lightweight detection [2] [3]. We have based our attack model on four types of DDoS attacks: Host scan, Port scan, TCP SYN flood, ICMP flood. Preliminary results show that the method is effective to extract the attack patterns and detect them. Following this introduction, the paper is organized as follows. Section 2 describes the previous work in the area of DDoS attack. Section 3 describes in detail, our proposed attack model methodology and detection method. Section 4 describes our experiments and results. Section 5 discusses limitation of the work, conclusion and future work.

II. RELATED WORK

A. *INTRUSION DETECTION SYSTEM (IDS)*

Intrusion detection system (IDS) has been extensively used to protect against the DDoS attacks. IDS detect attacks either by using signatures or anomaly behaviour. In signature based IDS, signatures of attack are matched to the traffic flow to identify the attack. In anomaly based IDS, deviation from normal system behaviour helps to detect an attack. The weakness of signature IDS is that it cannot detect new attack while anomaly IDS considers normal activity as malicious. Intrusion detection systems cause high level of resource consumption.

B. *BLINC[1]:-*

BLINC or BLINd Classification is an approach based on classification of traffic flows according to the applications that generate them. The method observes and identifies the patterns of host behaviour. The patterns are analysed at three

different levels namely a) the social level b) the functional level c) the application level. Analysing the traffic flows at different levels is the distinct feature of this approach.

The method is operated in dark means it does not access the packet payload, there is no knowledge of port numbers and only information about the current flow collectors is provided. There are two unique features of the method, first is that it focuses on classifying the individual flows to associating Internet hosts with applications and after that it classifies the flow accordingly. The authors believe that, by observing the host activity more information can be extracted and nature of applications of the host can be deduced. Second, BLINC analyses host behaviour at three different levels:

a) social level b) functional level c) application level

At the social level, host popularity is taken into consideration. The interactions of a host with other host are observed. Also, it identifies the host communities. At the functional level, the functional role of host in the network is considered, such as if the host is provider or consumer of a service or both. The role of a host is identified by observing the number of ports a single host uses for communication. For example: If a single port has been used by a host in number of interactions then BLINC assumes that the host provides a specific service. At the application level, transport layer interactions between hosts on specific ports are captured to identify the application of origin. For each application, the behaviour pattern is created in the form of graphlets. In BLINC classification, a set of predefined graphlets is matched with flow behaviours. The key feature of this methodology is tunability. The method gives results at different levels of detail with accuracy. BLINC first analyses traffic at three mentioned levels. Then a criterion for classification is controlled using thresholds which can be relaxed or tightened. There is a flexibility to choose level of accuracy and detail according to i) the goal of the study ii) the amount of exogenous information. The other highlights of the work are development of classification benchmark, identification of patterns of behaviour, highly accurate classification and detection of unknown attacks. The distinctness of BLINC is that it focuses on all flows generated by hosts. BLINC is advantageous in the sense that it identifies unknown applications such as malicious flows.

C. *Lightweight Detection[2]:-*

The lightweight detection technique is based on the Blind classification or BLINC [1]. In this work, DoS attacks are classified into four classes namely, SYN flood, ICMP flood, port scan and host scan. Here the attack pattern is described as graphlet. SYN flood, ICMP flood, and host scan graphlets are defined in this paper while the port scan graphlet is taken from BLINC [1]. Lightweight technique detects attack by comparing the traffic flow with the graphlets. In TCP SYN flood attack, the attacker sends a large number of TCP SYN packets with a spoofed source IP address. Since the target gets flooded with the half open connection its resources are consumed and it does not provide a normal service.

In ICMP flood attack, the attacker sends a large number of ICMP packets.

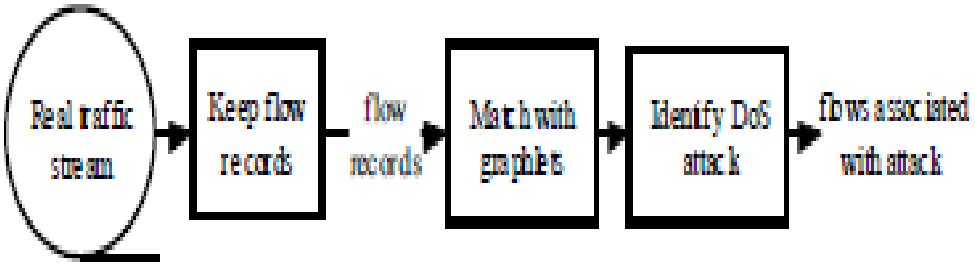

Fig 1. Flowchart for DoS detection [2]

This attack is detected by the large number of ICMP packets destined to the same IP address. Port scan and host scan are used as tools by the attacker to check the vulnerability of the systems. Host scan and port scan finds out the vulnerable target host and its port. Lightweight detection method is advantageous because of its light weight.

Without analysing the packet content, packet size, or packet inter- arrival time, it can identify the DoS activities.

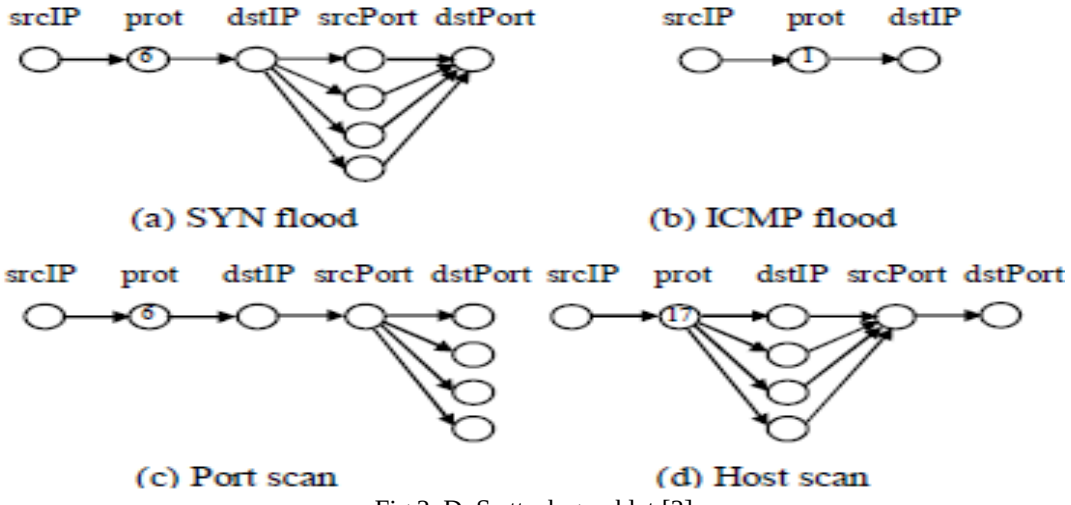

Fig 2. DoS attack graphlet [2]

D. *LD²[3]:-*

The LD² method proposes lightweight detection of DoS attacks. The system observes the flow behaviours and matches them with graphlets for each attack. The system is said to be lightweight as it does not analyses the packet such as its contents, size or statistics. Six types of DoS attacks is employed in this method such as SYN flood, ICMP flood, host scan, port scan, UDP flood and smurf. In LD² the effect of background traffic intensity is studied. Based on this study, appropriate threshold levels are defined. The performance of LD² work is benchmarked in terms of detection accuracy, CPU utilization and memory requirement. This method is based on the idea of BLINC. The system analyses and differentiates flow behaviours into graphlets of different attack types. A graphlet is defined as a signature which captivates the behaviour of a specific attack. Every graphlet depicts the relationship between source and destination ports usage, the sets of distinct ports and IPs. The LD² system observes attack activities for time interval of one minute. During each interval packets are captivated and differentiated into flows of five tuples namely srcIP, protocol, dstIP, srcPort, dstPort. All flow records are mapped to the graphlets at the end of the interval. If the graphlets matches, all flows of that graphlet are considered as attack activity. After this, the graphlet is removed from the system and the unmatched graphlets are carried forward for next analysis. For each type of attack there can be multiple graphlets since the graphlets are indexed by source IP addresses. The intensity of background traffic plays a major role in deciding the threshold of graphlet matching. The LD² is trained to recognize attack traffic at various intensity levels of background traffic to determine the threshold levels. Two types of background traffic traces namely controlled traces and real traffic traces are used.

The key advantage of LD² is that it detects rate based attack such as flooding attacks. Its flexibility recognizes abnormal traffic such as Trojans and worms. It consumes less memory. However, the disadvantage is that it cannot detect bad traffic except DoS and requires more CPU resources [4].

III. METHODOLOGY

In this section we describe our technique. Our proposed method for attack model is based on lightweight methodology [2] [3]. The attack model[5] [11] contains signatures or attack patterns of the four attacks namely host scan, port scan, TCP SYN flood, ICMP flood. The model helps to effectively differentiate between the attack flow and normal traffic. The attack patterns are extracted from traffic flow. In our work, we develop four attack models for each type of attack. The idea is to first generate an attack [6] [7] to observe it and then extract the patterns or features of the attack. Thus, for every attack a different model exists.

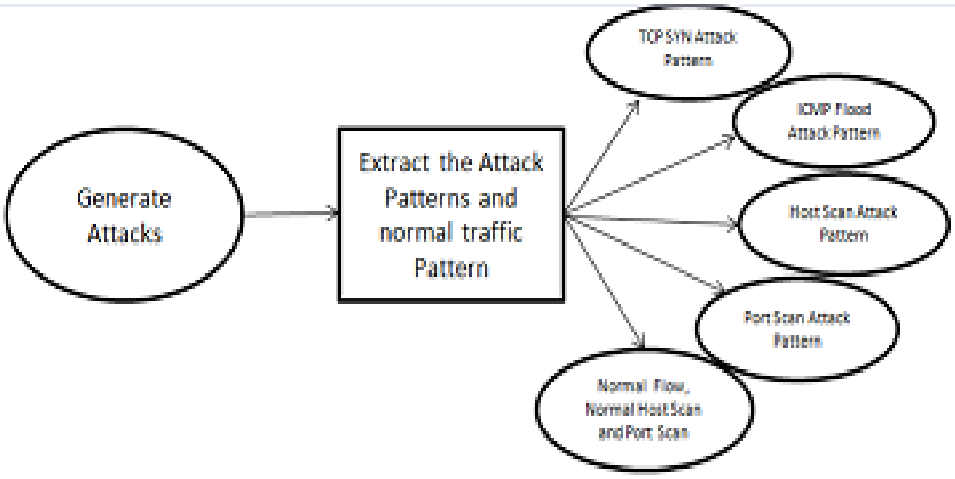

Fig 3. Attack Model Generation

For TCP SYN flood attack model, we first generate the TCP SYN flood attack, when the attack is generated we observe it and extract the pattern of the attack. In TCP SYN attack [6], the attacker sends SYN packet to the target with erroneous IP address. A SYN packet is used as a request to open a TCP connection. For every such request, the target will send SYN/ACK packet as a reply and tries to establish a TCP connection. These connections are never completed and they remain "half open" on account of spurious IP address of the attacker. The victim indefinitely waits for the reply of the attacker. As a result its resources are depleted while legitimate connections are denied. Thus, we can say that SYN flood attack has occurred if different numbers of source ports or source IPs are seen in the attack model. The attack is implemented by making modifications in the TCP SYN packet header unlike [2] [3]. We increment the sequence number of the packets, so that wrong sequence numbered packets are delivered to the victim and it waits indefinitely to complete the connection.

In ICMP flood attack [6], the attacker sends a large number of ICMP packets to the victim. Thereby, the target gets flooded with packets depleting the data transmission capacity for legitimate traffic. Thereby, in ICMP attack model, there is a continuous flow of packets. This attack is implemented by making changes in the ICMP packet header unlike [2] [3]. A counter is setup in the packet header which increments and floods the victim with a large number of packets.

In host scan attack model, we fix a threshold value. If the number of times of the scan surpasses the threshold value, then host scan attack is generated. However, if the numbers of scans are within the threshold limit it will not be

considered as an attack but a normal host scan activity. Host scan attack is generated by sending ICMP packets. Attacker sends a packet to a host, if a reply comes then it symbolizes that the host is active. Then data packets are sent to establish connection with the victim and to extract the required information of the host.

In port scan attack model, ports are scanned using a threshold value. If the ports are scanned beyond the threshold value it is indicated as an attack. However, if it is scanned below threshold value it is considered as normal activity. Port scanning informs which ports are active and services provided by them [12]. The active ports are scanned a number of times to extract more information such as port number, destination IP address and services provided [8].

Basically, host scan and port scan do not impose any threat to the systems. They are carried out to check the vulnerability. After that, the attacks are launched by the attacker. The common tuple which is used in all the four models is sourceIP address. Other tuples vary according to the nature of the attacks.

Thus, we have developed four attack models which distinguish between the normal traffic flow and attack traffic flow.

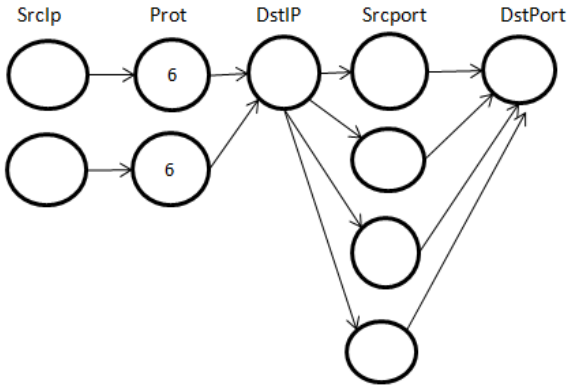

Fig 4. Attack Model for TCP SYN Flood

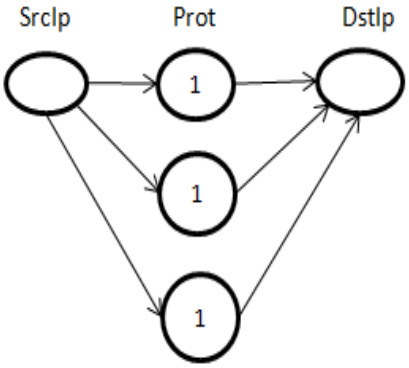

Fig 5. Attack Model for ICMP

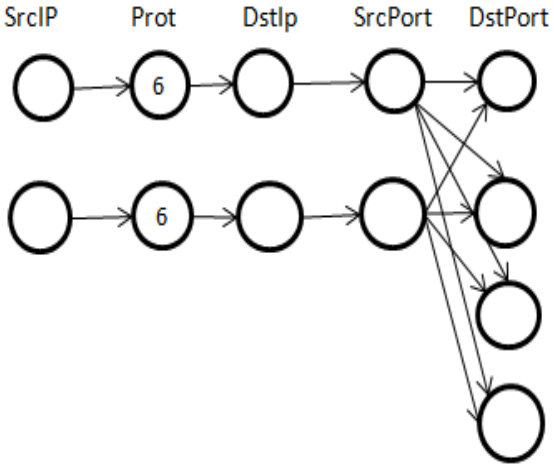

Fig 6. Attack Model for Port Scan

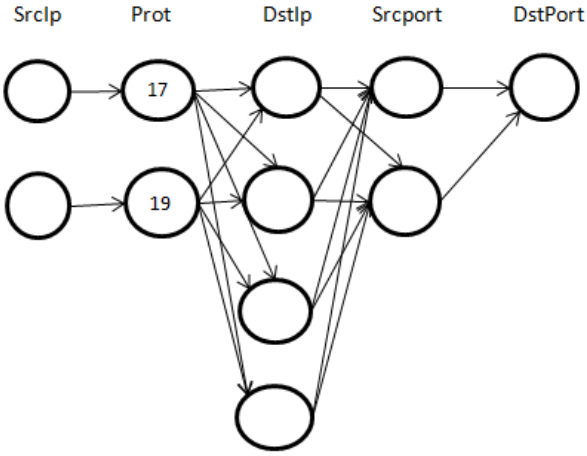

Fig 7. Attack Model for Host Scan

Detection of D DoS Using Attack Model

Each type of attack is detected by comparing flow behaviours against the attack models.

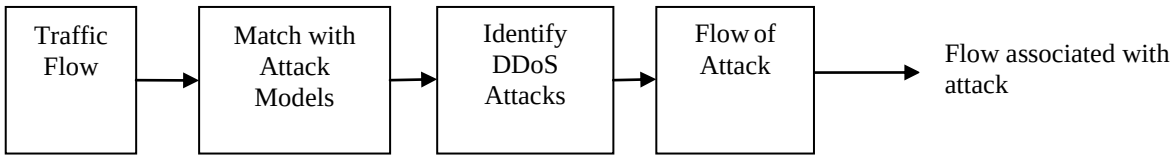

Fig 8. Flowchart for DDoS Detection

Our detection method has three steps: The *traffic flow* module captures the traffic flow based on 5-tuple flow records (srcIP, protocol, dstIP, srcPort, and dstPort) and sends flow records to the *Match with Attack Model module*, which maps each flow record to pre-defined attack model. Finally, the *Identify DDoS attack* module uses predefined threshold value to identify flows associated with DDoS activities. Flows that match with one of the model are then classified as DDoS traffic. The model that has been classified in each interval will be removed from memory. The flows classified as DDoS attack will be kept for future reference. Any unclassified pattern will be considered as unknown. The key advantage of the proposed method is its lightweight. It can identify a group of hosts associated with DDoS activities without analyzing packet content, packet size. Furthermore, our technique can detect other network anomaly if they pose similar behaviours as these DDoS attacks.

IV. EXPERIMENTAL RESULTS

In this section we describe our results using network simulator.

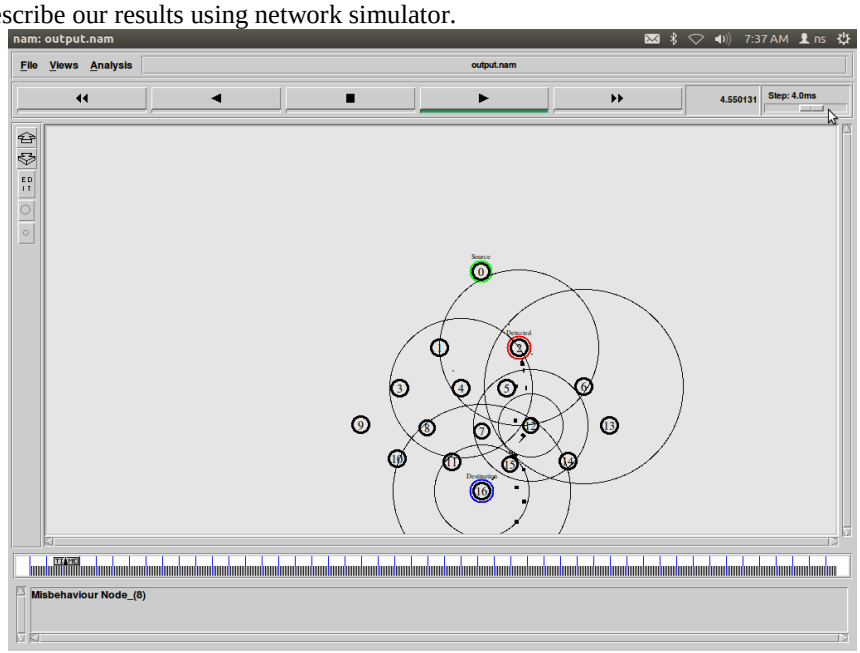

Fig 9. Host Scan Detection

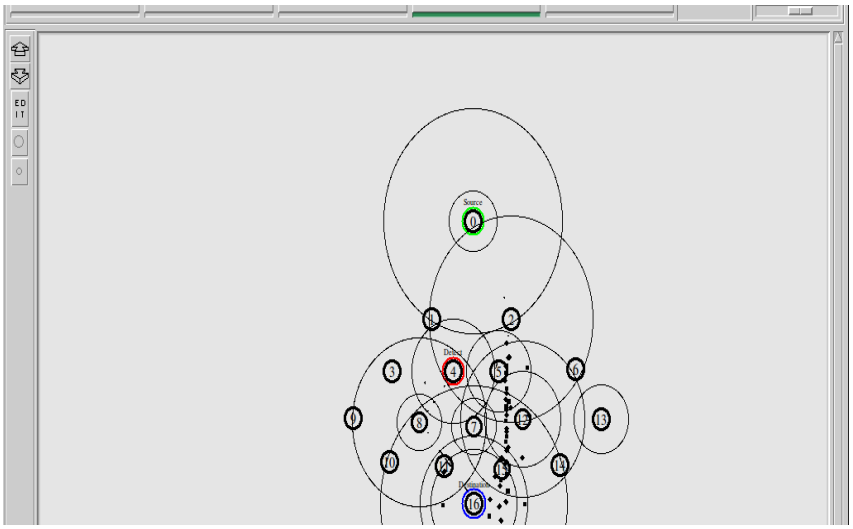

Fig 10. Port Scan Detection

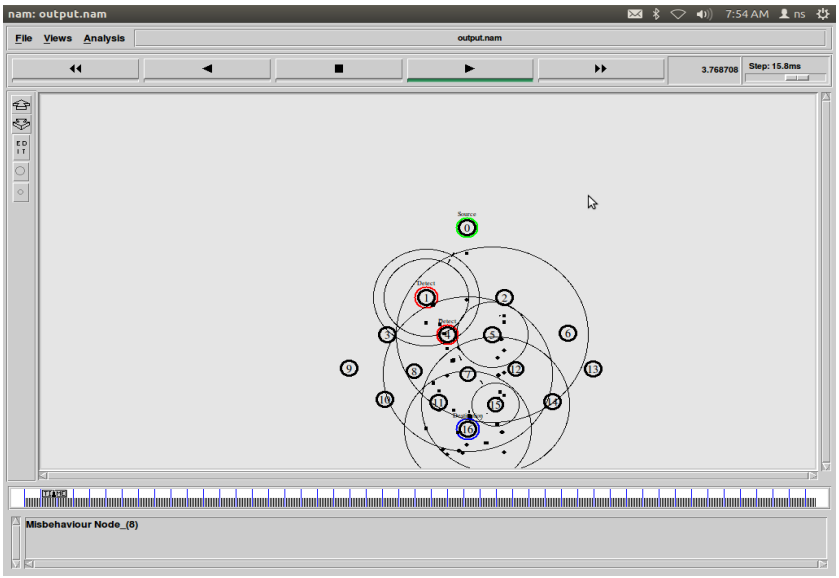

Fig 11. ICMP Flood Detection

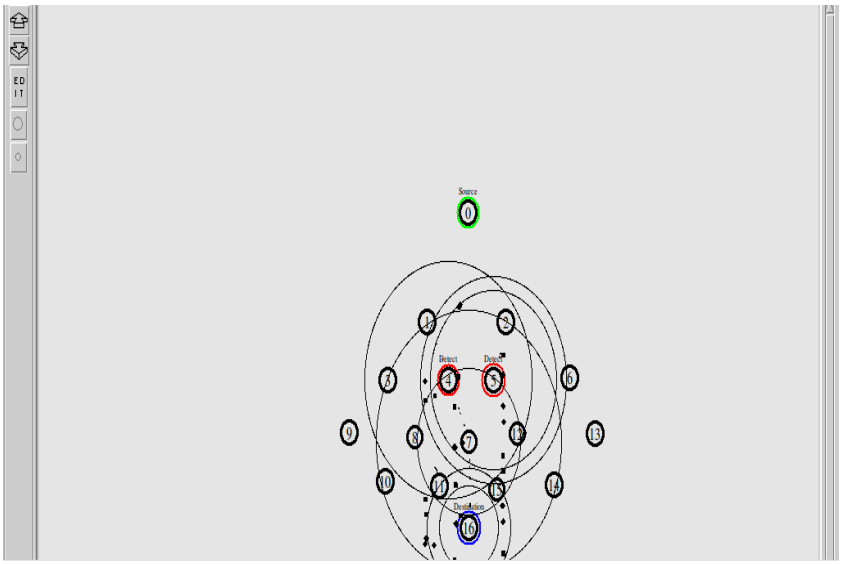

Fig 12. TCP SYN Flood Detection

The Fig 9 depicts the host scan detection. Fig 10 depicts the port scan detection. Fig 11 depicts the ICMP detection. Fig 12 depicts TCP SYN Flood attack.

V. CONCLUSION

We propose attack models for the four DDoS attack. The model extracts the attack patterns for the host scan attack, port scan attack, TCP SYN flood attack, ICMP flood attack. The model is generated in two steps, first we generate the attacks and secondly we extract the attack patterns on the basis of their flow behaviour. The advantage of the method is that we can effectively differentiate between a normal flow and attack flow. For generation of attack models we need to have prior knowledge about the nature and characteristics of the attacks. The model identifies attack flow but it cannot identify the specific attack except those mentioned above. The Detection of attacks is done by comparing the attack models with the traffic flow. If the flow matches with any particular attack model then that particular attack is detected [9] [10] [11].

REFERENCES

[1] Thomas Karagiannis, Konstantina Papagiannaki, and Michalis Faloutsos, "BLINC: Multilevel Traffic Classification in the Dark," ACM Sigcomm, 2005.

[2] Sirikaran Pukkawanna, Vasaka Visoottiviseth, Panita Pongpaibool" Lightweight Detection of DoS Attacks "In Proc of IEEE ICON 2007, Adelaide, South Australia, November 2007.

[3] Sirikaran Pukkawanna, Panita Pongpaibool, Vasaka Visoottiviseth, "LD2: A System for Lightweight Detection of Denial of Service Attacks"IEEE 2008.

[4] Snort, http://www.snort.org.

[5] Jie Yu, Zhoujun Li, Huowang Chen, Xiaoming Chen "A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks" Third International Conference on Networking and Services (ICNS'07).

[6] Jelena Mirkovi´c, Gregory Prier, Peter Reiher," Attacking DDoS at Source".

[7] J. Mirkovic, J. Martin, and P. Reiher, "A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms," ACM Sigcomm Computer Comm. Rev., vol. 34, no.2, 2004, 39–53.

[8] Cynthia Bailey Lee, Chris Roedel, Elena Silenok, "Detection and Characterization of Port Scan Attacks".

[9] Theerasak Thapngam, Shui Yu, Wanlei Zhou, Gleb Beliakov,"Discriminating DDoS Attack Traffic from Flash Crowd through Packet Arrival Patterns" First International Workshop on Security in Computers, Networking and Communications, IEEE 2011.

[10] Simona Ramanauskaitė1, Antanas Čenys, "Composite DoS Attack Model ", ISSN 2029-2341 print / ISSN 2029-2252, Vilniaus Gedimino technikos universitetas.

[11] Jalal Atoum, Omar Faisal, "Distributed Black Box and Graveyards Defense Strategies against Distributed Denial of Services", Second International Conference on Computer Engineering and Applications (ICCEA), 2010.

[12] Cynthia Bailey Lee" Detection and Characterisation of Port Scan Attacks".

