Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 9, September 2013, pg.286 – 295

RESEARCH ARTICLE

A Random Mechanism to Measure and Predict Changes in DDos Attacks

Hemanth Siramdasu[1], Premnath G[2], Karthick M[3]

[1]Computer Science & Engineering, VelTech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

[2]Computer Science & Engineering, VelTech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

[3]Computer Science & Engineering, VelTech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India

[1] hemanth204@gmail.com; [2] prem_nathcse@yahoo.co.in; [3] pthick@gmail.com

Abstract— Distributed Denial-of-Service (DDoS) attacks are a vital menace to the Internet. Nevertheless, the recollection take away attribute of the Internet routing methods builds it particularly inflexible to draw back to the resource of these assaults. Because of these, there is no helpful and proficient technique to pact with this concern up to at hand. In this study, we recommend an innovative map out process for DDoS attacks that is supported on randomness of flow of packets in among common and DDoS attack transfer, which is primarily unlike from generally used packet spotting practices. In association to the active DDoS draw back techniques, the projected approach encloses a number of benefits as memory non severe, capably scalable, vigorous beside packet contamination, and self-governing of attack traffic models.

Keywords— **Packet filtering; overload control; system design; Distributed denial of service (DDoS) attacks; Detection**

I. Introduction

It is a strange face up to trackback the basis of Distributed Denial-of-Service (DDoS) attacks in the Internet[1]. In DDoS attacks, attackers engender a massive sum of requests to fatalities from side to side compromised computers (zombies), in the midst of the intend of refuse usual examine or corrupting of the excellence of services[2]. It has been a foremost hazard to the Internet since years, and a current analysis on the prime Internet operators in the world established that DDoS attacks are growing severely, and individual attacks are stronger and refined. Additionally, the review moreover set up with the intention of the crest of 40 gigabit DDoS attacks almost doubled in 2008 contrast with the earlier year[3]. The major grounds behind this occurrence is to facilitate the network security community does not have useful and capable sketch back methods to situate attackers as it is effortless for attackers to masquerade themselves by taking compensation of the vulnerabilities of the World Wide Web, such as the vibrant, stateless, and unidentified character of the Internet.

IP trackback way the competence of identifying the authentic resource of any packet sent athwart the Internet[4]. For the reason that of the susceptibility of the novel proposes of the Internet, we could not be able to uncover the authentic hackers at current. In actual fact[5], IP trace back methods are measured thriving if they can recognize the zombies starting which the DDoS attack packets entered the Internet. Study on DDoS detection, improvement, and filtering has been conducted pervasively. Though, the work on IP trace back is inadequate. A number of IP trackback approaches have been elective to classify attackers and there are two foremost methods for IP trackback, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM). A serious hazard to the Internet is Distributed Denial of Service (DDoS) attack. At present, the majority ISPs simply depend on physical detection of DDoS attacks subsequent to which offline superior particle traffic study is carried out and latest filtering policies are installed by hand to the routers[6]. The requirements of human involvement consequences in meager response time and fall short to look after the sufferer ahead of brutal damages are recognized[7].

The articulacy of existing filtering policies is too partial and unyielding while compared to the ever-evolving uniqueness of the offensive packets[8]. Newly, we have proposed DDoS defense structural design that ropes scattered finding and mechanized on-line attack categorization. In this work, we will spotlight on intend and assessment of the preset attack categorization, discerning packet disposal and surplus control segment of the projected structural design[9]. Our vital design is to prioritize packets by support on for every packet attains which approximates the authority of a packet specified the characteristic values it consists. Particular concern is made to make sure that the method is agreeable to high-speed hardware accomplishment[10]. When the score of a packet is computed, we carry out score-based choosy packet throwing away where the dropping threshold is dynamically adjusted based on the score allocation of current inward packets and the present point of overload of the scheme.

II. LITERATURE SURVEY

Conventionally, the approach in use to attacks is to examine the stuffing of each packet. Though, packet scrutiny cannot simply be conducted at high-speeds. Consequently, researchers and operators are in progress of investigating substitute approaches, such as flow-based intrusion detection. In that method the stream of data in the course of the network is examined, as a substitute of the data of each entity packet[11]. Packet Score has been projected as a practical DDOS resistance method, which notices DDOS attacks, distinguishes attack packets from genuine ones with the employ of packet scoring, and junks packets whose scores are minor than a dynamic threshold. Additionally, a leaky-bucket overflow manage method abridges the score calculation, and make possible high-speed accomplishment. An attribute-value-variation scoring format examines the divergence of the existing traffic attribute values, and boosts the exactness of noticing and distinguishing attacks[12].

An improved control-theoretic packet throwing away scheme permits both methods to be additional adaptive to demanding attacks such as those with not varying signatures and intensities. When collective as one, the proposed extensions not only seriously condense the memory necessity and performance difficulty but also considerably progress the accuracies in attack detection and packet differentiation. This makes ALPi an attractive DDOS defense system amenable for high-speed hardware accomplishment[13]. As novel countermeasures are developed to avoid DDOS attacks, attackers are continuously increasing innovative manner to avoid these new countermeasures[14]. Attack lessening formats dynamically strangle attack traffic produced in Distributed Denial-of-Service (DDOS) attacks. Attack Diagnosis (AD) merges the idea of Pushback and packet marking, and its structural design is in line with the ultimate DDOS attack countermeasure standard attack recognition is conducted next to the victim host and packet sort out is carried out near to the attack sources[15]. AD is a reactive defense mechanism that is activated by a victim host after an attack is detected. By instructing its upstream routers to mark packets deterministically, the victim can trace back one attack source and command an AD-enabled router close to the source to filter the attack packets[16]. This process isolates one attacker and throttles it, which is repeated until the attack is mitigated. We also propose an extension to AD called Parallel Attack Diagnosis (PAD) that is able of throttling traffic coming from a large number of attackers simultaneously. Client puzzles have been projected in a numeral of protocols as a method for extenuating the effects of disseminated denial of service (DDOS) attacks. In sort to offer shield against concurrent attacks transversely a ample choice of applications and protocols, conversely, such puzzles should be located at a layer regular to every of them; the network layer. Inserting puzzles at the IP layer basically modifies the service pattern of the Internet, permitting some device inside the network to shove load back on top of those it is servicing[17]. A benefit of network layer puzzles above earlier puzzle systems is that they can be useful to all traffic from spiteful clients, building it probable to preserve alongside random attacks and making before intended mechanisms compulsory.

III. EXISTING SYSTEM

It is an extraordinary challenge to trackback the source of Distributed Denial-of-Service (DDOS) attacks in the Internet. A number of IP trackback approaches have been suggested to identify attackers and there are two major methods for IP trackback, the probabilistic packet marking (PPM) and the deterministic packet marking (DPM)[18]. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network) where the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot trackback to the attack sources located out of the ISP network. The DPM strategy requires all the Internet routers to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability of DPM is a huge problem. Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers[19]. Further, both PPM and DPM are vulnerable to hacking, which is referred to as packet pollution.

A. Disadvantages

1. There is no effective and efficient method to deal with this issue so far.
2. It is infeasible in practice at present.
3. Work depends heavily on traffic patterns to conduct their trackback.

IV. PROPOSED SYSTEM

In this study we propose a novel trackback method for DDOS attacks that is based on entropy variations between normal and DDOS attack traffic, which is fundamentally different from commonly used packet marking techniques .IP trackback means the capability of identifying the actual source of any packet sent across the Internet. In fact IP trackback schemes are considered successful if they can identify the zombies from which the DDOS attack packets entered the Internet. IP trackback methods should be independent from packet pollution and various attack patterns. Entropy rate, the entropy growth rate as the length of a stochastic sequence increases, was employed to find the similarity between two flows on the entropy growth pattern, and relative entropy, an abstract distance between two probabilistic mass distributions, was taken to measure the instant difference between two flows. My proposed method can work independently as an additional module on routers for monitoring and recording flow information, and communicating with its upstream and downstream routers when the pushback procedure is carried out. The proposed method can archive real time trackback to attackers. Once the short term flow information is in place at routers, and the victim notices that it is under attack, it will start the trackback procedure. The workload of trackback is distributed, and the overall trackback time mainly depends on network delays between the victim and the attackers.

B. Overview Of Ppm And Dpm

Both of these strategies require routers to inject marks into individual packets. Moreover, the PPM strategy can only operate in a local range of the Internet (ISP network), where the defender has the authority to manage. However, this kind of ISP networks is generally quite small, and we cannot trace back to the attack sources located out of the ISP network. The DPM strategy requires all the Internet routers to be updated for packet marking. However, with only 25 spare bits available in as IP packet, the scalability of DPM is a huge problem. Moreover, the DPM mechanism poses an extraordinary challenge on storage for packet logging for routers. Therefore, it is infeasible in practice at present. Further, both PPM and DPM are vulnerable to hacking, which is referred to as packet pollution. IP trackback methods should be independent of packet pollution and various attack patterns.

C. Entropy Rate

Entropy rate, the entropy growth rate as the length of a stochastic sequence increases, was employed to find the similarity between two flows on the entropy growth pattern, and relative entropy, an abstract distance between two probabilistic mass distributions, was taken to measure the instant difference between two flows. In this project, I propose a novel mechanism for IP trace back using information theoretical parameters, and there is no packet marking in the proposed strategy; we, therefore, can avoid the inherited shortcomings of the packet marking mechanisms. We categorize packets that are passing through a router into flows, which are defined by the upstream router where a packet came from, and the destination address of the packet. During non attack periods, routers are required to observe and record entropy variations of local flows. In this study, we use flow entropy variation or entropy variation interchangeably.

D. Advantages

1) In comparison to existing DDOS trackback methods, the proposed strategy possesses a number of advantages - it is memory non-intensive, efficiently scalable, robust against packet pollution and independent of attack traffic patterns.
2) The results of extensive experimental and simulation studies are presented to demonstrate the effectiveness and efficiency of the proposed method.
3) My experiments show that accurate traceback is possible within 20 seconds (approx.) in a large scale attack network with thousands of zombies.
4) The proposed strategy overcomes the inherited drawbacks of packet marking methods, such as limited scalability, huge demands on storage space and vulnerability to packet pollutions .
5) The proposed method will be effective for future packet flooding DDOS attacks because it is independent of traffic pattern.

V. Modules

E. Module description

There are four modules in this study are as follows:

1) *Topology Creation:* This module is used to construct the topology. Now create the Unstructured Network Connection for transfer the data in different network for communication, then create the number of local area network topology for local communication, then create the router, in which router maintains all transferring client details and this transferring data and their packets, then followed by creation of different nodes, server and router in proper name, IP Address and port number for data communication, below figure shows the creation of topology

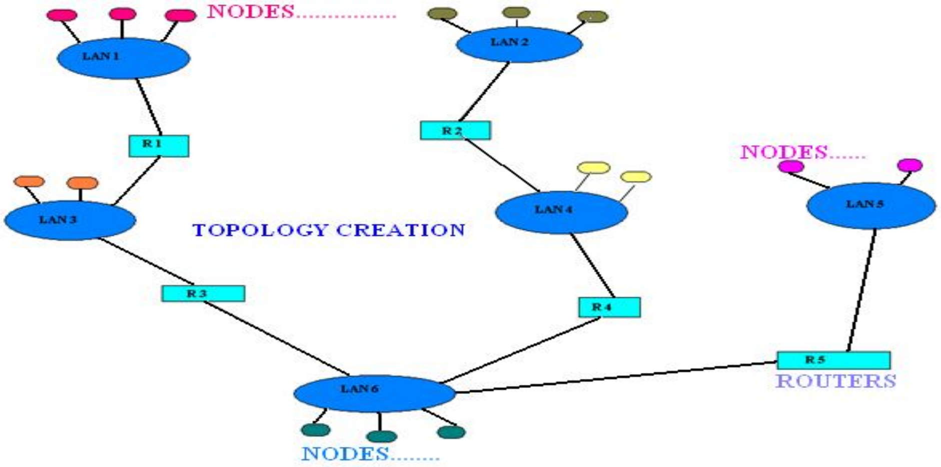


Fig 1.Topology Creation

2) *DDos Attack:* The attacker(s) first establishes a network of computers that will be used to generate the huge volume of traffic needed to deny services to legitimate users of the victim. The attackers discover vulnerable hosts on the network. The next step for the attacker is to install new programs (known as attack tools) on the compromised hosts of the attack network. The hosts running these attack tools are known as zombies, numerous zombies together form an army or botnet. There are two categories of DDoS attacks, Typical DDoS attacks and Distributed Reflection Denial-of-Service (DRDOS) attacks. In a typical DDoS attack, the master computer orders the zombies to run the attack tools to send huge volume of packets to the victim, to exhaust the victim's resources. Unlike the typical DDoS attacks, the army of a DRDOS attack consists of master zombies, slave zombies, and reflectors. The difference in this type of attack is that slave zombies are led by master zombies to send a stream of packets with the victim's IP address as the source IP address to other uninfected machines (known as reflectors), exhorting these machines to connect with the victim. Then the reflectors send the victim a great volume of traffic, as a reply to its exhortation for the opening of a new connection, because they believe that the victim was the host that asked for it.

3) *Entropy variations*: Compared with the non-attack situation, the entropy of a local router drops dramatically when attack flows are passing the local router. For a local router on an attack path, the entropy variation of the output flows is not greater than the summation of the entropy variation of the incoming flows. The entropy variation drops when a local router is closer to the victim and vice versa. Based on the partial information of the attack that the traceback algorithms have accumulated, we can estimate the number of zombies to be traced and the maximum length to the most far away zombies. There are no attackers at the upstream routers if a local router's entropy variation is reasonable. The number of flows for a given router is stable at both the attack cases and no attack cases. There are two algorithms in the proposed traceback suite, the local flow monitoring algorithm and the IP traceback algorithm. The local flow monitoring algorithm is running at the no attack period, accumulating information from normal network flows, and progressive the mean and the standard variation of flows.
4) *IP Traceback*: Once a DDOS attack has been confirmed by any of the existing DDOS detection algorithms, then the victim starts the IP traceback algorithm. Then, the probability of a packet marked by a router d that hops away from the victim Based on the number of marked packets, we can reconstruct the attack path. However, it requires large number of packets to improve the accuracy of the attack path reconstruction. Therefore, an edge sampling algorithm was proposed to mark the start router address and end router address of an attack link and the distance between the two ends.

F. Data Flow Diagram

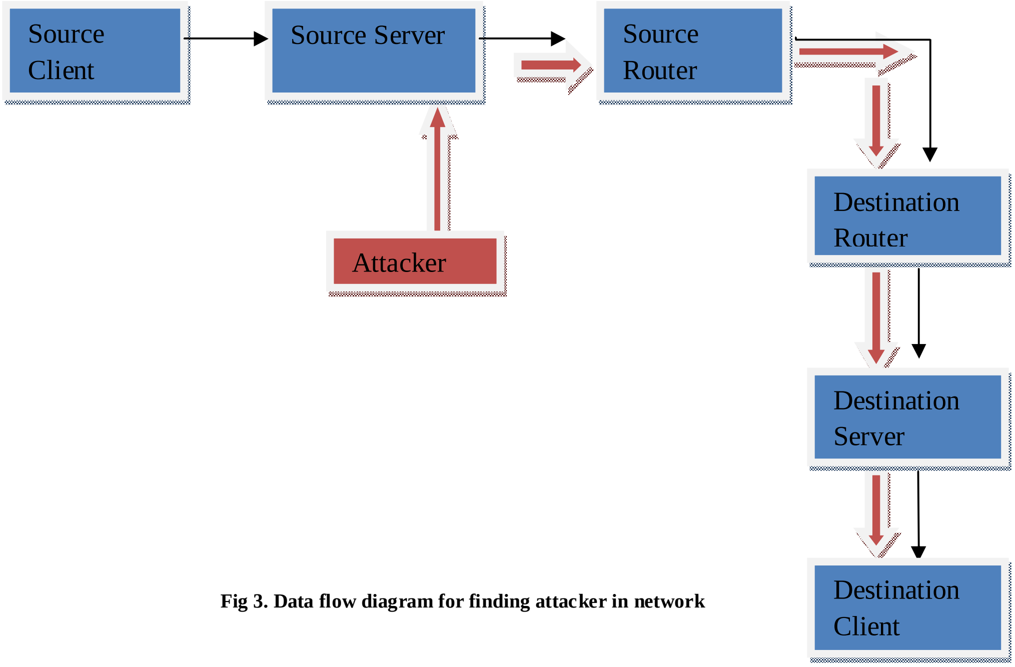
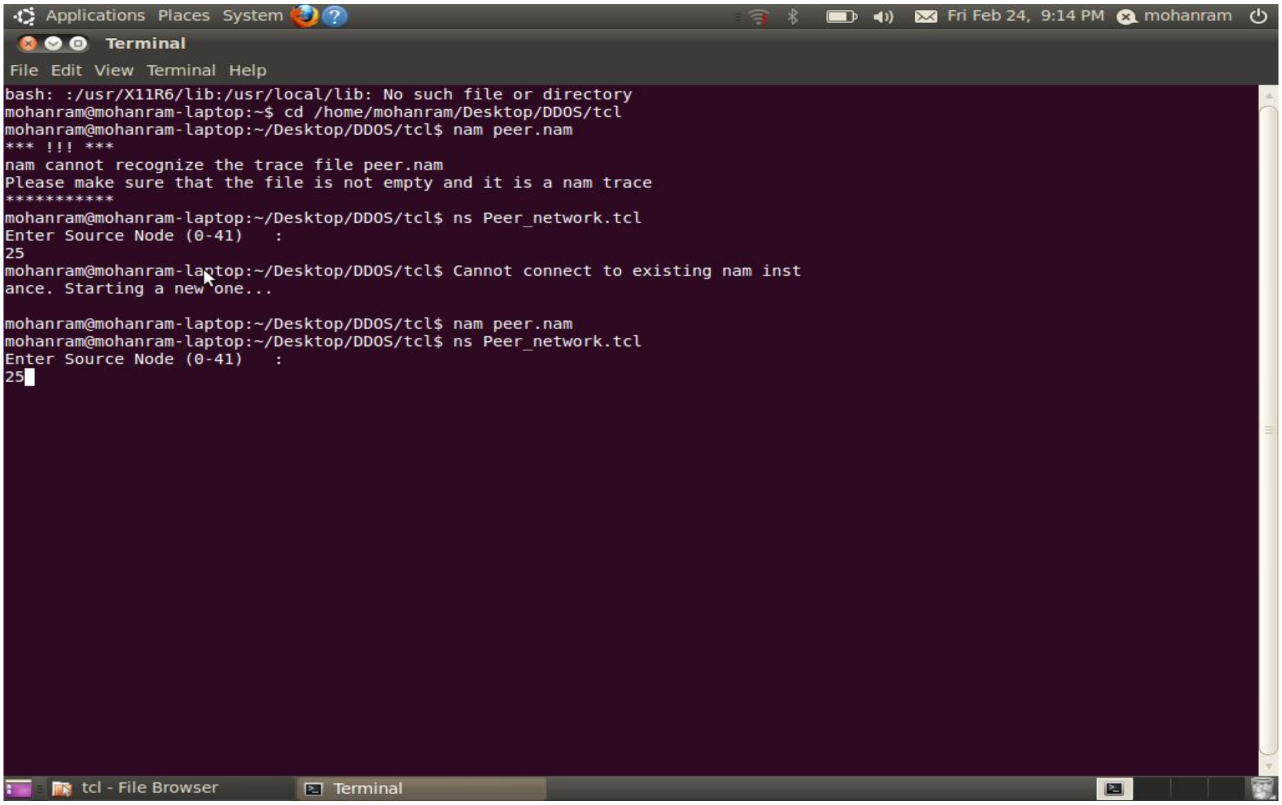


Fig 3. Data flow diagram for finding attacker in network

VI. SIMULATION RESULTS

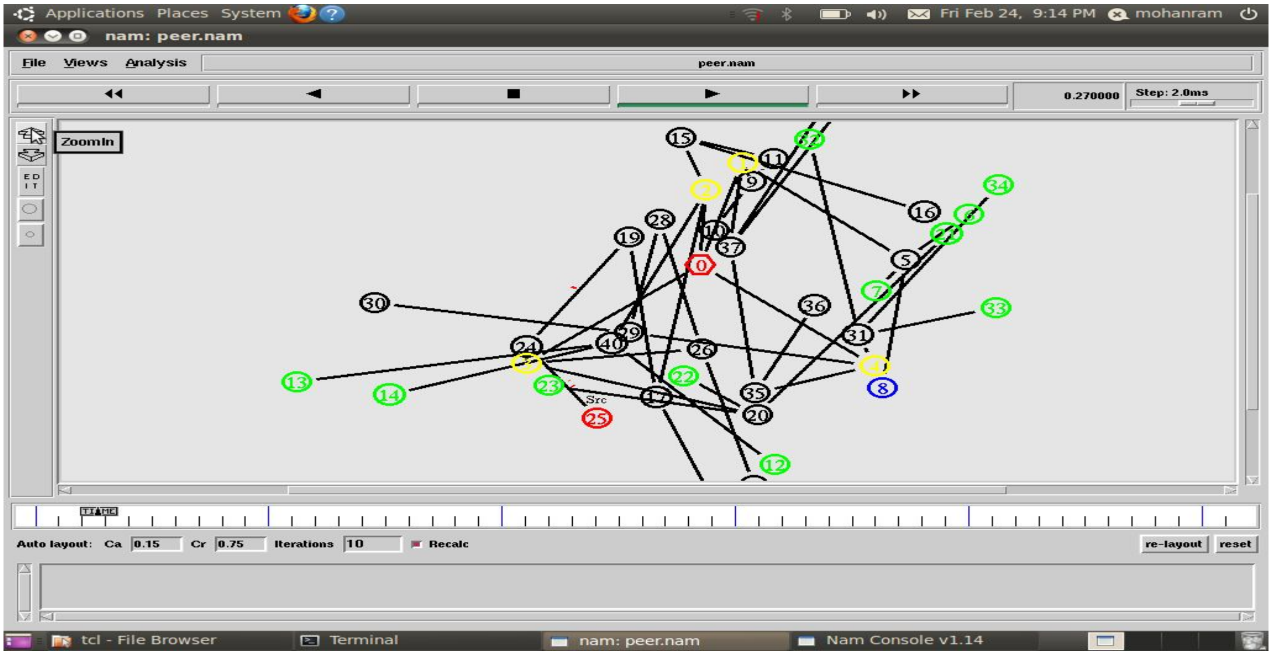
G. Giving the file location and source node name.


Applications Places System
Fri Feb 24, 9:14 PM mohanram
Terminal
File Edit View Terminal Help
tcl - File Browser
Terminal

```
bash: :/usr/X11R6/lib:/usr/local/lib: No such file or directory
mohanram@mohanram-laptop:~$ cd /home/mohanram/Desktop/DDOS/tcl
mohanram@mohanram-laptop:~/Desktop/DDOS/tcl$ nam peer.nam
*** !!! ***
nam cannot recognize the trace file peer.nam
Please make sure that the file is not empty and it is a nam trace
***********
mohanram@mohanram-laptop:~/Desktop/DDOS/tcl$ ns Peer_network.tcl
Enter Source Node (0-41)    :
25
mohanram@mohanram-laptop:~/Desktop/DDOS/tcl$ Cannot connect to existing nam inst
ance. Starting a new one...

mohanram@mohanram-laptop:~/Desktop/DDOS/tcl$ nam peer.nam
mohanram@mohanram-laptop:~/Desktop/DDOS/tcl$ ns Peer_network.tcl
Enter Source Node (0-41)    :
25
```

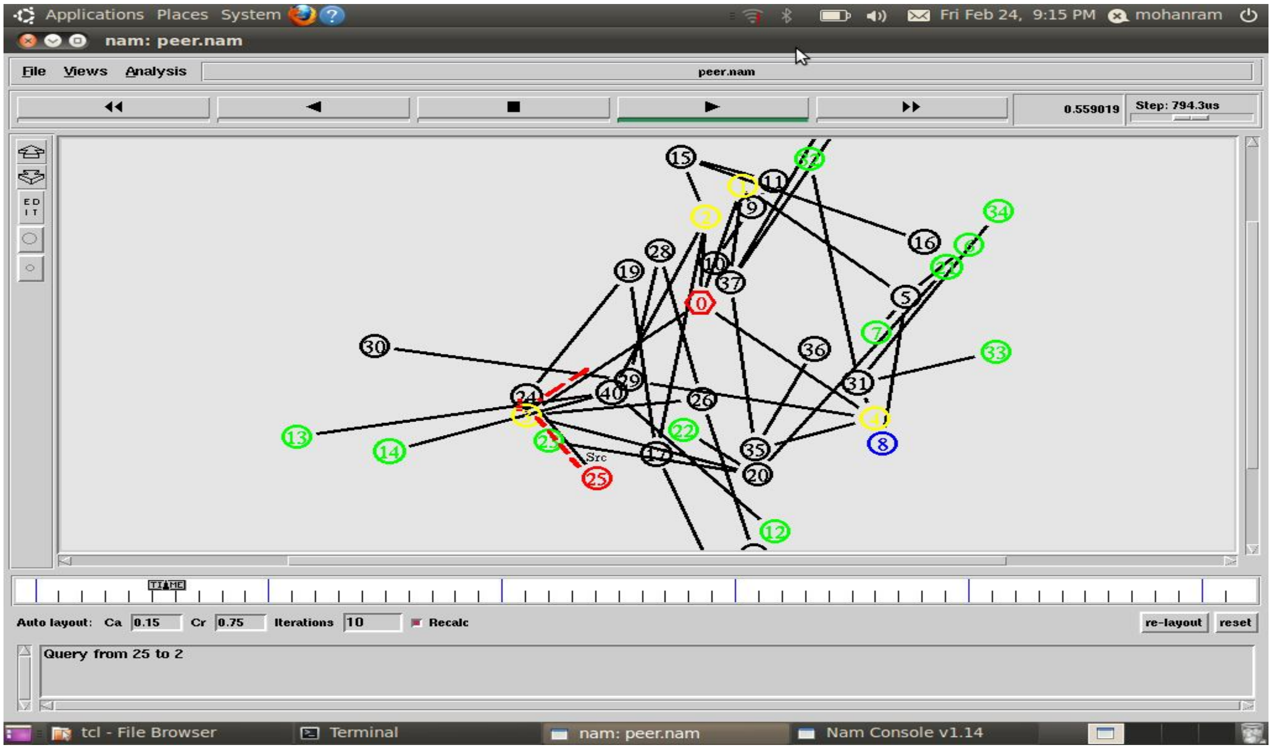
H. Source node is 25



0.270000 Step: 2.0ms

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc

I. Destination node is 2 and source node chooses the path node

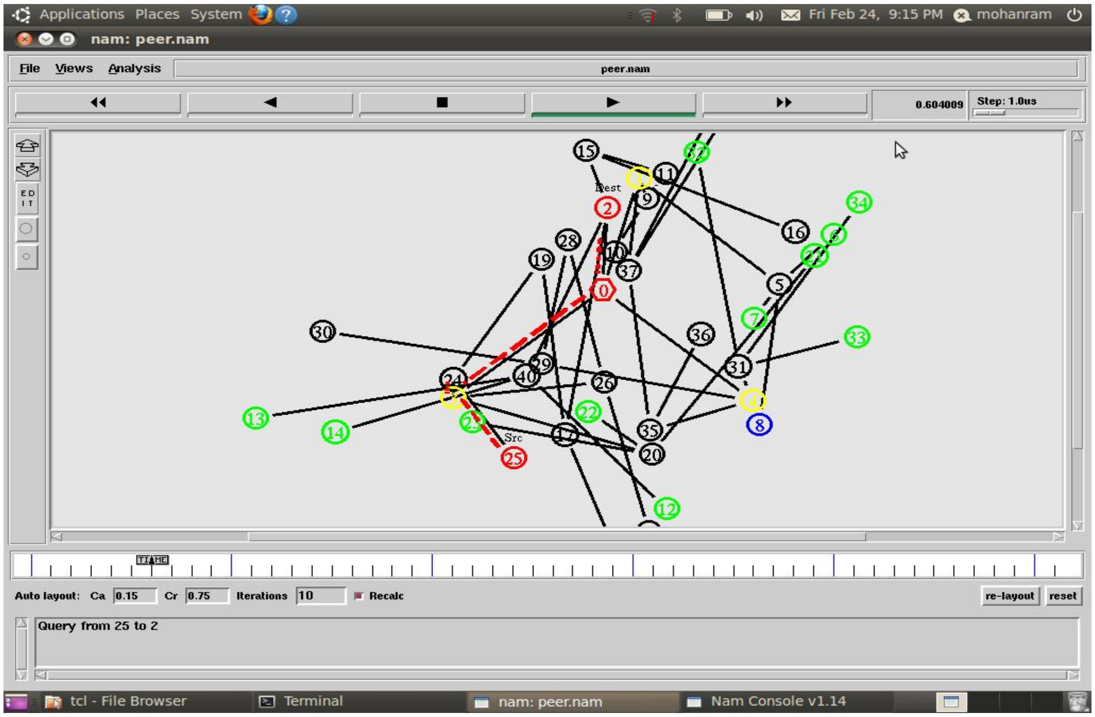

Applications Places System
Fri Feb 24, 9:15 PM mohanram
nam: peer.nam
File Views Analysis
peer.nam
EDIT
15 32 1 11 9 2 34 16 6 28 10 37 19 5 27 0 7 30 36 33 31 24 40 29 26 3 8 13 14 23 22 35 17 Src 25 20 12
TIME
re-layout reset
tcl - File Browser Terminal nam: peer.nam Nam Console v1.14

0.559019 Step: 794.3us

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc

Query from 25 to 2

J. Data packets transfers from source node to destination node using path nodes

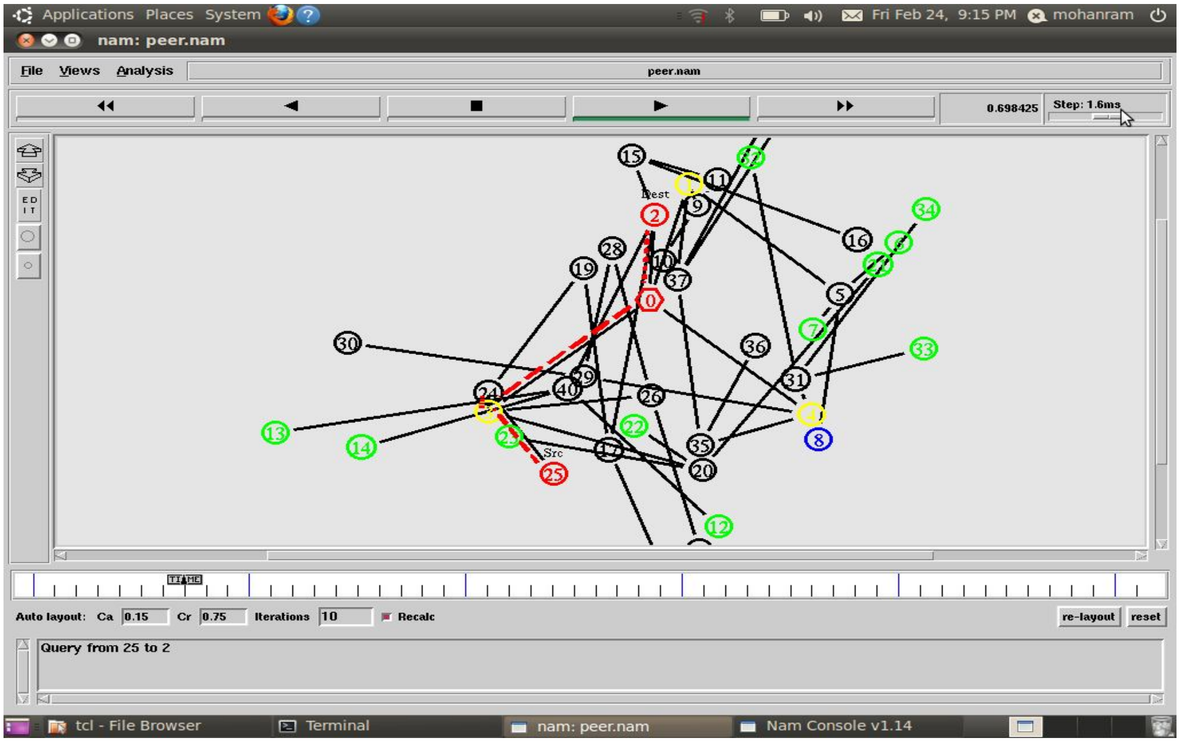

Applications Places System
Fri Feb 24, 9:15 PM mohanram
nam: peer.nam
File Views Analysis
peer.nam
EDIT
15 32 1 11 Dest 9 2 34 16 6 28 10 37 19 5 27 0 7 30 36 33 31 24 40 29 26 3 8 13 14 23 22 35 17 Src 25 20 12
TIME
re-layout reset
tcl - File Browser Terminal nam: peer.nam Nam Console v1.14

0.604009 Step: 1.0us

Auto layout: Ca 0.15 Cr 0.75 Iterations 10 Recalc

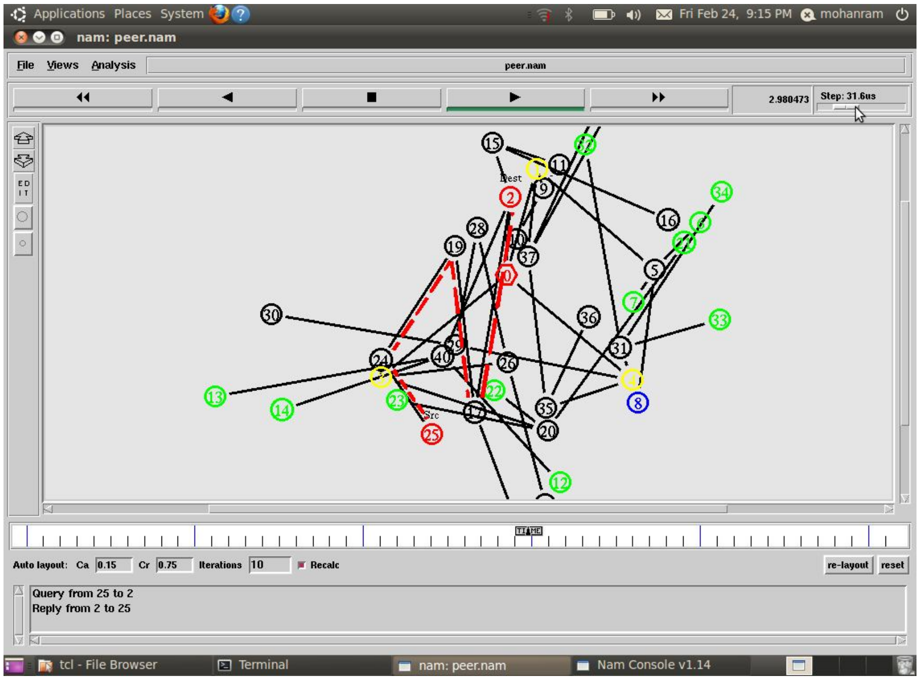
Query from 25 to 2

K. DDos attacks takes place during transfer of packets from source to destination.



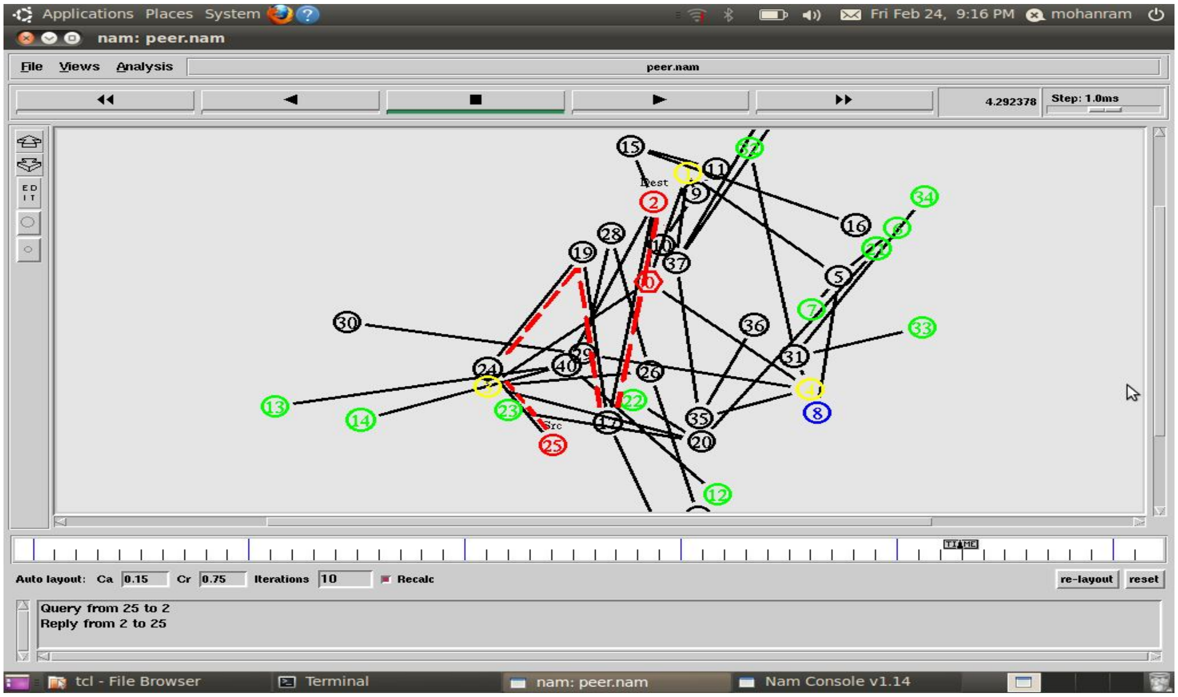
```
0.698425   Step: 1.6ms
Auto layout:  Ca 0.15   Cr 0.75   Iterations 10   Recalc
Query from 25 to 2
```

L. Trackback is done from destination to source by sending the reply data packets.



```
2.980473   Step: 31.6us
Auto layout:  Ca 0.15   Cr 0.75   Iterations 10   Recalc
Query from 25 to 2
Reply from 2 to 25
```

M. False packets are determined and deleted by using the intermediate nodes



```
Query from 25 to 2
Reply from 2 to 25
```

VII. CONCLUSION

In this study, we proposed an effective and efficient IP traceback scheme against DDOS attacks based on entropy variations. It is a fundamentally different traceback mechanism from the currently adopted packet marking strategies. Many of the available work on IP traceback depend on packet marking, either probabilistic packet marking or deterministic packet marking. Because of the vulnerability of the Internet, the packet marking mechanism suffers a number of serious drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on storage space at victims or intermediate routers. On the other hand, my proposed method needs no marking on packets, and therefore, avoids the inherent shortcomings of packet marking mechanisms. It employs the features that are out of the control of hackers to conduct IP traceback. I observe and store short-term information of flow entropy variations at routers. Once a DDOS attack has been identified by the victim via detection algorithms ,the victim then initiates the pushback tracing procedure. The traceback algorithm first identifies its upstream routers where the attack flows came from, and then submits the traceback requests to the related upstream routers.

REFERENCES

[1] Kevin J. Houle. “Trends in Denial of Service Attack Technology”. *CERT Coordination Center, Carnegie Mellon Software Engineering Institute.* Oct 2001.

[2] Tao Peng, Ramamohanarao, “*Survey Of Network-Based Defense Mechanisms Countering The Dos And Ddos Problems*” ACMJ258-03 ACM-CSUR 2007.

[3] PyungKoo Park, Daejeon,Et.al, “*Service-Oriented DDoS Detection Mechanism Using Pseudo State in a Flow Router” International Conference on Information Science and Applications (ICISA)*, June 2013.

[4] Vassilakis, V.G. ; Reed, M.J, “*Mitigating brute-force attacks on Bloom-filter based forwarding” Conference on Future Internet Communications (CFIC)*, 2013.

[5] D. Yau, J. Lui, F. Liang, and Y. Yam. *Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. IEEE/ACM Transactions on Networking*, 13(1), February 2005.

[6] Ruiping Lua, Kin Choong Yow, “*Mitigating DDoS attacks with transparent and intelligent fast-flux swarm network” IEEE Transactions on Networking*, June 2011.

[7] Zargar, S.T, Joshi, J, Tipper, D, “*A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, Communications Surveys & Tutorials, IEEE* (Volume:PP , Issue: 99), 2013.

[8] Soon Hin Khor ; NICT, Tokyo, Japan ; Nakao, A, "*DaaS: DDoS Mitigation-as-a-Service" IEEE/IPSJ 11th International Symposium on Applications and the Internet (SAINT),* 2011.

[9] Chen, Yonghong, Ma, Xinlei ; Wu, Xinya," *DDoS Detection Algorithm Based on Preprocessing Network Traffic Predicted Method and Chaos Theory" Communications Letters, IEEE (Volume:17 , Issue: 5),* 2013.

[10] Soundar Rajam, V.K. Shalinie, S.M." *A novel traceback algorithm for DDoS attack with marking scheme for online system" Recent Trends In Information Technology (ICRTIT), International Conference on* April 2012.

[11] Durcekova, V, Schwartz, L. ; Shahmehri, N, '*Sophisticated Denial of Service attacks aimed at application layer" ELEKTRO,* May 2012.

[12] Thapngam, T, Shui Yu ; Wanlei Zhou," *DDoS discrimination by Linear Discriminant Analysis (LDA) "International Conference on Computing, Networking and Communications (ICNC),* Feb 2012.

[13] Soon Hin Khor, Nakao, A, "Overfort: Combating DDoS with peer-to-peer DDoS puzzle" *IEEE International Symposium on Parallel and Distributed Processing, IPDPS* April 2008.

[14] Fei Wang ; Xiaofeng Hu ; Jinshu Su," *Unfair rate limiting for DDoS mitigation based on traffic increasing patterns", IEEE 14th International Conference on Communication Technology (ICCT),* Nov 2012.

[15] Jin-Seok Yang ; Min-Woo Park ; Tai-Myoung Chung," *A Study on Low-Rate DDoS Attacks in Real Networks "International Conference on Information Science and Applications (ICISA),* June 2013.

[16] Lei Liu ; Xiaolong Jin ; Geyong Min ; Li Xu," *Real-Time Diagnosis of Network Anomaly Based on Statistical Traffic Analysis" IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom),* June 2012.

[17] Michalas, A. ; Komninos, N. ; Prasad, N.R. ; Oleshchuk, V.A., "*New client puzzle approach for DoS resistance in ad hoc Networks" IEEE International Conference on Information Theory and Information Security (ICITIS),* Dec 2010.

[18] Alenezi, M. ; Reed, M.J., "*Efficient AS DoS traceback" International Conference on Computer Applications Technology (ICCAT),* Jan 2013.

[19] You-ye Sun ; Cui Zhang ; Shao-qing Meng ; Kai-ning Lu," *Modified Deterministic Packet Marking for DDoS Attack Traceback in IPv6 Network, "IEEE 11th International Conference on Computer and Information Technology (CIT), Sep* 2011.