Grid High Availability and Service Security Issues with Solutions

Muhammad Zakarya, Muazzam Ali Khattak, Izaz Ur Rahman, and Ayaz Ali Khan

***Abstract*—DDoS attacks are launched through sending a large quantity of packets to a target machine, using instantaneous teamwork of multiple hosts which are distributed throughout the Grid computing environment. Today DDoS attacks on the Internet in general and especially in Grid Computing environment has become a visible issue in computer networks. DDoS attacks are easy to generate but their detection is a very difficult task and therefore, an attractive weapon for hackers. DDoS streams do not have familiar characteristics, therefore currently available IDS cannot detect these attacks perfectly. Similarly, there implementation is a challenging task. In practice, Gossip based DDoS attacks detection mechanism is used to detect such types of attacks in network, by exchanging traffic over line. Gossip based techniques results in network congestion and have overhead of extra packets. Keeping the above drawbacks in mind, we are going to propose a DDoS detection and prevention mechanism, that has the beauty of being easy to adapt and more reliable than existing counterparts. We are going to introduce entropy based detection mechanism for DDoS attack detection. Our proposed solution has no overhead of extra packets, hence resulting in good QoS. Once DDoS is detected, any prevention technique can be used to prevent DDoS in Grid environment.**

***Index Terms*—Normalized entropy (NE), denial of service (DoS), grid simulator (GridSim).**

I. Introduction and Concepts

Grid Computing, more specifically computational grids is the application of several systems to a single huge problem at the same time, usually to a scientific or technical problem that needs a large number of CPU processing cycles i.e. more CPU power or access to huge and large amounts of data. One of the main Grid Computing strategies is to use different softwares to divide and apportion different pieces of a single program among several individual systems, may be up to many thousands [25]. These systems, taking part in Grid System are called nodes. Grids are called super computers for economically poor organizations. The GS consists of GN and a GNM. When multiple GS are combined in such a way, that at least one of them registers its available services to a Broker as shown in Fig. 1. And others Grid Sites (GS) requests for such registered services from the Broker. The Environment is called Grid Computing Environment.

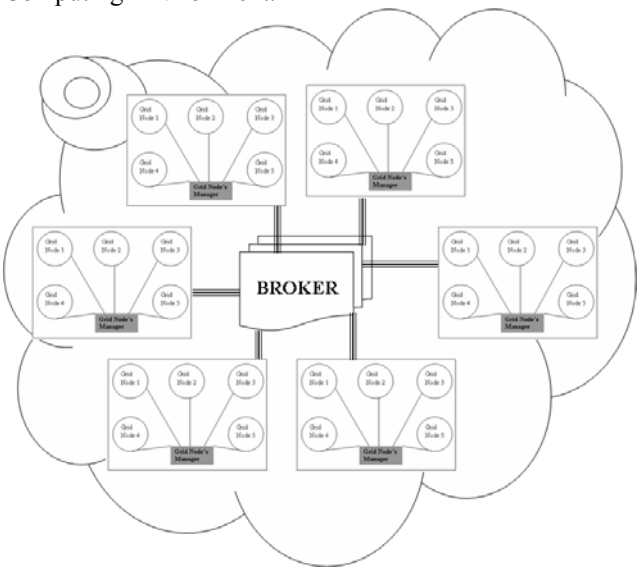

Fig. 1. The grid computing environment

A. HA in Grid Systems

Any system which is always available to its customers is HA. High availability of grid system can be achieved, through implementing a lot of architectures. For example reduce congestion. It is difficult to achieve HA in today's global village because more services are required to customers. The more congested the network, more systems are offline to its customers. Considering TCP congestion scenario, where TCP drops all extra packets resulting in increased queuing delays. Therefore using traditional TCP congestion detection, avoidance mechanisms are not to achieve HA.

B. QoS in Grid Environment

We are trying to study different service level security issues in Grid computing especially in wireless grids, and will try to propose new solutions to their security improvements. As service level security issues like DoS Attacks & Network Congestion, are most important. Solving these issues results in High Availability as well as. In high available systems, QoS services are expected from service providers.

C. Security Issues

As networks are coming common to layperson in computer technology, the need to provide good services to its customers at any time is essential. Grid computing provides its services to its customers on need basis, means whenever, what is required must be provided. Therefore managing QoS and making the systems available, each and every time, to provide its services to Grid users and customers, is a must.

Manuscript received September 28, 2012; revised November 2, 2012.

Muhammad Zakarya and Muazzam Ali Khattak are with Department of Computer Science, Abdul Wali Khan University, Mardan, Pakistan (e-mail: mohd.zakarya@awkum.edu.pk, muazzam@awkum.edu.pk).

Izaz Ur Rahman is with Department of Computing & Mathematics, Brunel University, London, UK (e-mail: izaz.rahman@brunel.ac.uk).

Ayaz Ali Khan is with COMSATS Institute of Information Technology, Islamabad, Pakistan (e-mail: ayazak12345@gmail.com).

DOI: 10.7763/IJET.2012.V4.472

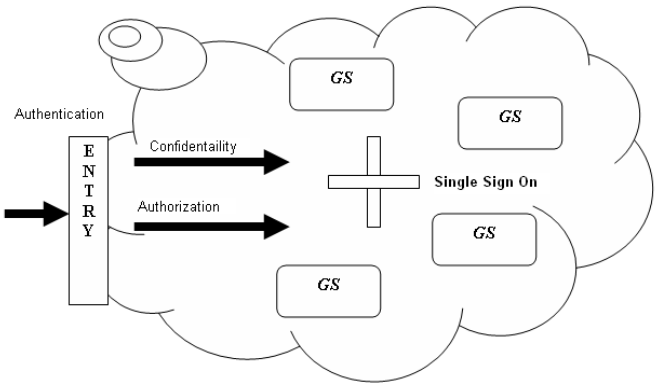

Fig. 2. Security model for grid computing environment

D. Distributed DoS Attack

DDoS attacks are launched by sending a large volume of packets to a target machine, using simultaneous cooperation of multiple hosts which are distributed throughout the Grid computing environment. Mostly DDoS attacks are considered as congestion control problem. DDoS attacks are two phases attack. In first phase the attacker finds some vulnerable systems in the network. The attacker install some DDoS tools on these systems, also called zombies or agents. In second phase all zombies create the actual attack on the victim, as shown in Fig. 3 below [2].

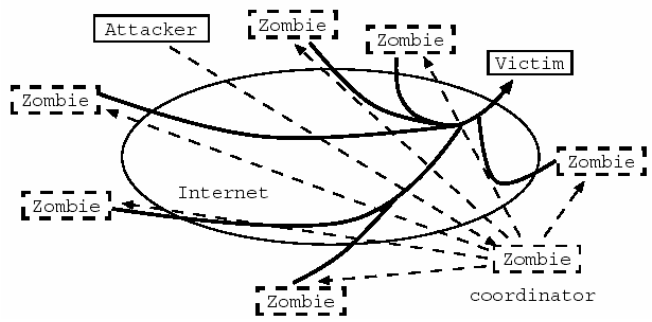

Fig. 3. Attacker, zombies and victims [2]

E. IP Spoofing

Change of source address in the header of an IP packet is called IP Spoofing. It requires privileged access to network stack (raw socket access). A partial solution to IP Spoofing is to associate a fixed MAC address with each IP address in a subnet to detect spoofing.

II. Related Work and Existing Techniques

In this section we discuss some existing mechanisms and techniques.

A. Mutually Guarded Approach

In wireless communication medium, if a node-A (attacker) (masquerade itself as node-B), sends packets to node-C, where nodes A & B are in the same coverage area, then that packet will also be received by node-B. Therefore node-B will easily catch the attack. But if nodes B & C are in different coverage area or both nodes B & C are out of range to each other, in that scenario the attacker will successfully launch its attack, as shown in Fig. 4.

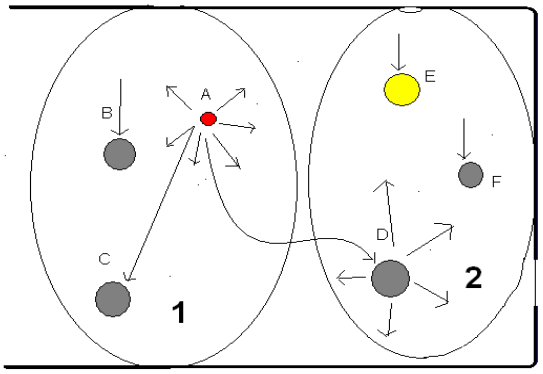

Fig. 4. Mutually guarded approach

B. Ingress & Egress Filtering

Ingress & Egress filtering mechanism is shown diagrammatically in Fig. 5 [10].

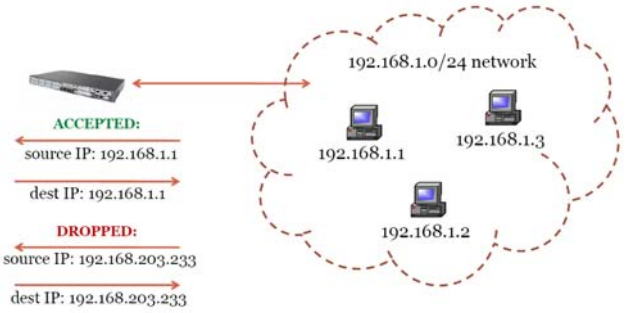

Fig. 5. Ingress and egress filtering [10]

C. IP Trace-back Mechanism

In this technique the attacker is traced, by location. Actually without any mobility, it is some what easy, but when mobility is involved, the attacker cannot be traced easily.

D. Distributed Change Point Detection (DCD)

In [6] the authors have proposed a new detection mechanism for DDoS. A CAT is constructed. Nodes in a CAT are ATRs that participate in forwarding the malicious flows. The links in the CAT indicate the path along which attacking traffic goes towards the victim. Once a CAT is constructed, a DDoS attack is detected and ATRs are identified. The next task is to filter out malicious flows.

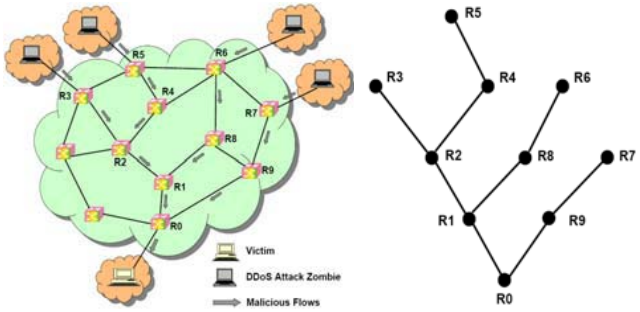

Fig. 6. IP Trace-back mechanism [6]

E. Moving Target Defense

A Band-Aid solution to a DDoS attack is to change the IP address of the victim computer, thereby invalidating the old address. The technique may work in some cases but administrators must make a series of changes to DNS entries, routing table entries etc.

F. Rate Limiting

Rate-limiting mechanisms compel a rate limit on a set of packets that have been characterized as nasty by the detection mechanism. It is a moderate response technique that is usually deployed when the detection mechanism has many false positives or cannot accurately illustrate the attack flow.

G. Mitigating DDoS Attacks via Attestation (Assayer)

In [9] the authors have proposed a new hardware based attestation mechanism to detect and prevent DDoS attacks. On a per-packet basis, they proposed to provide the network with the dominant ability to identify, the code on the end host that generated or permitted the packet. The story is shown in Fig. 7 below.

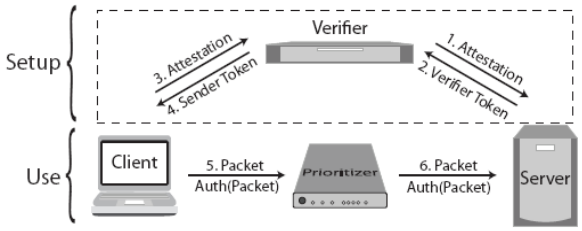

Fig. 7. Assayer [9]

H. Traffic Shaping

A number of routers available in the bazaar today have features that permit you to limit the amount of bandwidth that some specific type of traffic can consume. This is occasionally referred to as "traffic shaping" technique [10].

I. Internet Protocol Ver 6 (IPv6)

IPv.4 does not have any check or methods to authenticate whether the IP address i.e. source address, that the sender puts into an IPv.4 packet header field, is justifiable or not. As a result, the authentication of source IP address is to be anticipated to enhance and improve an Internet Security against current DoS attacks as shown in Fig. 8 [10].

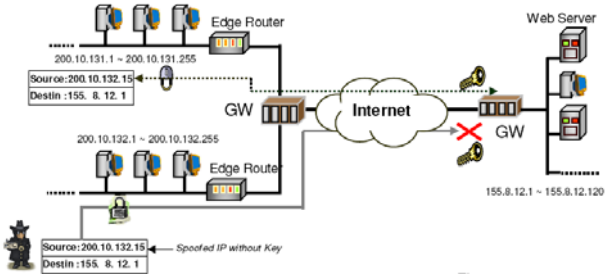

Fig. 8. IP version 6

III. Existing Problem

We are going to propose a DDoS detection and prevention mechanism, that has the beauty of being easy to adapt and more reliable than existing counterparts. As, in service level security issues DoS Attacks, DDoS & Network Congestion, are most important. Solving the issue of DDoS also results in High Availability as well as good QoS.

IV. Proposed Solution

After a deep study of available techniques, we are going to introduce a new IDS, which can be implemented on our own proposed architecture, resulting in DDoS detection and prevention mechanism.

A. Proposed Architecture

In our proposed architecture, we have divided the whole Grid System into regional areas i.e. GS, where each GS is protected by an AS / GL. Our developed ADS is installed on two places i.e. every Grid Node & AS or on their respective routers. A packet which is detected as cruel once at AS, is marked out, so that Client node can be informed. In our proposed architecture (for future direction), DDoS source is detected for future prevention. A tree is maintained at every router, by marking every packet with path modification strategy, so that the victim is able to trace the sender of the packet. Any packet which was detected as malicious flow, can be confirmed in a second try i.e. confirmation process at GN i.e. victim node. In phase 1 we detect malicious flow, while in phase 2 we have a confirmation algorithm so either to drop the attack flow, or to pass it otherwise. In the given scenario, we consider that AS is configured properly for policed address i.e. the attacker node address or victim IP address.

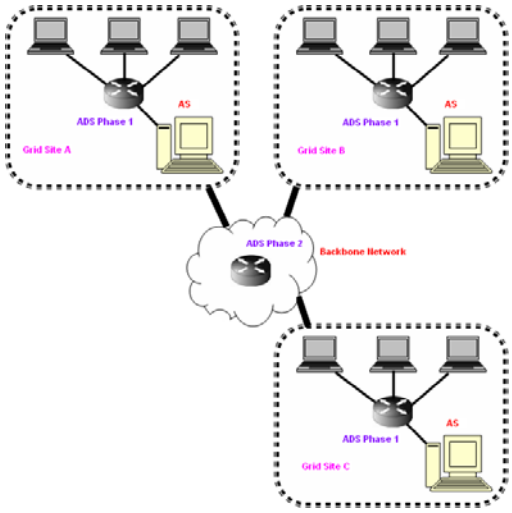

Fig. 9. Proposed grid architecture

- Authentication Server (AS) or Geographical Authentication & Authorization Server (GAS) is responsible for controlling the geographical area where defined.
- Locally phase 1 is executed & at the core router phase 2 takes place.

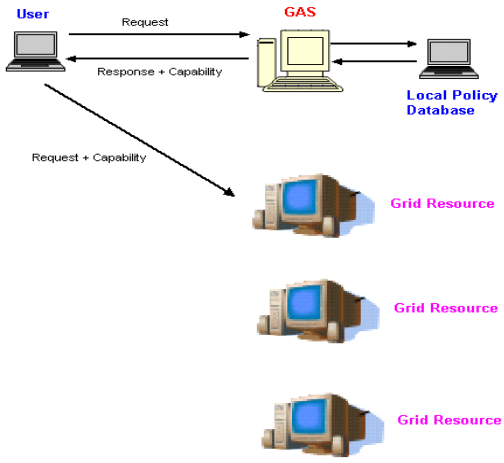

Fig. 10. Working diagram of proposed grid architecture

PROS & CONS

- Local Security Policy
- Little computation as compared to Global security policy
- Near the source detection
- No overhead of extra packet
- User accesses GAS, authenticated & authorization check
- Performance Scalability + load balancing + QoS
- No need for resources to check the user identity
- Local & Quick allocation of resources by GAS
- No Single point of failure, affect some part of the Grid
- GAS are required to inform all corresponding GAS in case of new node to any geographical community
- GAS is attacked by DDoS, not possible

B. Intrusion Detection System

IDS may be in software form and/or in hardware form, that will monitor the network for disbelieving activity and alerts the network administrator to take a particular action accordingly. Signature based IDS will observe packets on the network and judge against them to a database maintained with well-known threats. On the other hand, using an ADS, if deviation of user activity is exterior a certain threshold value, it is marked as nasty and a reaction is triggered. After a deep survey of DDoS detection & prevention mechanism we reach to the point that Entropy may be used as DDoS detection metric.

C. Information Theory & Entropy based ADS

According to [14], any statements that have some surprise and meaning are called information. Some consider that information theory is to be a subset of communication theory, but we consider it much more. The word entropy is rented from physics, in which entropy is a measure of the chaos of a group of particles i.e. 2nd law of thermodynamics. If there are a number of possible messages, then each one can be expected to occur after certain fraction of time. This fraction is called the probability of the message. In [23], [24] Shannon proved that information content of a message is inversely related to its probability of occurrence. To summarize, the more unlikely a message is, the more information it contains. *In* [15], Entropy H(X) is given by

$$H(X) = -\sum_{x \in X} p(x) \log p(x)$$

The log is to the base 2 and entropy is expressed in bits. To say randomness is directly proportional to entropy i.e. more random they are, more entropy is there. The value of sample entropy lies between 0 and log(n). The entropy value is smaller when the class distribution belongs to only one & same class while entropy value is larger when the class distribution is more even. Therefore, comparing entropy values of some traffic feature to that of another traffic feature provides a mechanism for detecting changes in the randomness. We use traffic distribution like IP Address & application Port Number i.e. (IP address, Port). If we wants to calculate entropy of packets at a single or unique source i.e. destination, then maximum value of n must be 2^{32} for IPV4 address. Similarly if we want to gauge entropy at multiple application ports then value of n is the total number of ports [16]. In similar way, $p(x)$ where $x \in X$, is the probability that X takes the value x. We randomly examine X for a fix time window (w), then $p(x) = m_i/m$ Where, m_i is the total number we examine that X takes value x i.e

$$m = \sum_{i=1}^{n} mi$$

Putting these values in entropy equation 1, we get

$$H(X) = -\sum_{i=1}^{n} (m_i / m) \log(m_i / m)$$

Similarly, if we want to calculate the probability p(x), then m is the entire number of packets, but m_i is the number of packets with value x at destination as source [26]. Mathematically given as

$$p(x) \frac{\text{Number of packets with } x_i \text{ as source(destination)address}}{\text{Total number of peckets}}$$

Again if we want to calculate probability $p(x)$ for each destination port, then

$$p(x) \frac{\text{Number of packets with x as source(destination)port}}{\text{Total number of peckets}}$$

Remember that total number of packets is the number of packets observed in a specific time slot (w). When this calculation finishes, normalized entropy is calculated to get the overall probability of the captured flow in a specific time window (w). Normalized Entropy is given by

$$\text{Nomalized entropy} = (H / \log n_0)$$

where n_o is the number of dissimilar values of x, in a specific time slot (w). During the attack, the attack flow dominates the whole traffic, resulting in decreased normalized entropy. To confirm our attack detection, again we have to calculate the entropy rate i.e. growth of entropy values for random variables, provided that the limit exists, and is given by

$$H(X) = \lim_{n \to \infty} \frac{1}{n} H(x_1, x_2 \ldots x_n)$$

V. PROPOSED ALGORITHMS

For Detection of Ddos Attack

- Decide a threshold value δ_1
- On edge routers collect traffic flows for a specific time window (w)
- Find probability $P(X)$ for each node packets
- Calculate link entropy of all active nodes separately
- Calculate $H(X)$ for routers using Equation (1)
- Find normalized entropy using Equation (3)

  If normalized entropy < δ_1, identify malicious attack flow

For confirmation of attack flows

- Decide a threshold value δ_2
- Calculate entropy rate on edge router using Equation (4)

- Compare entropy rates on that router, if =< δ_2, DDoS confirmed
- Drop the attack flow

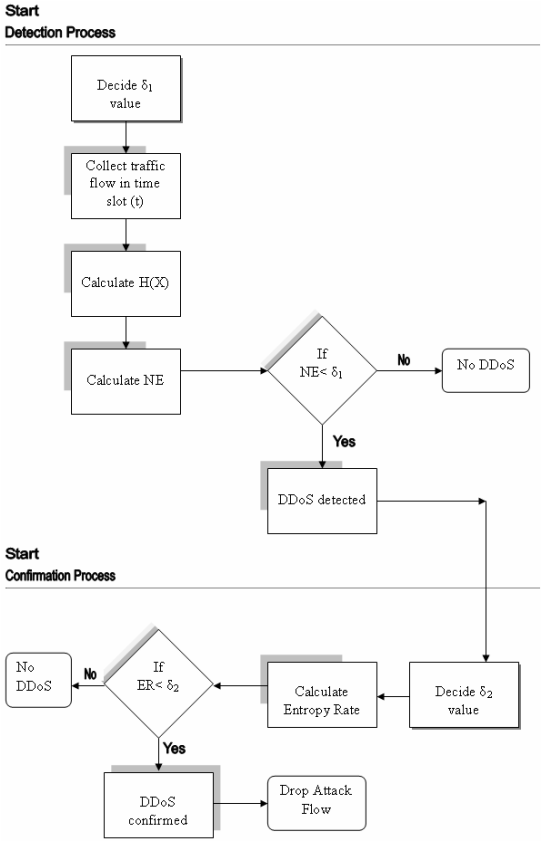

Fig. 11. Flow / transition diagram

VI. Implementation, Simulation & Results

In this section we describe that how to mathematically or statically implement our proposed scheme, while in section coming after that we have shown our simulation results along with charts form with a practical environment.

A. Mathematical Proof

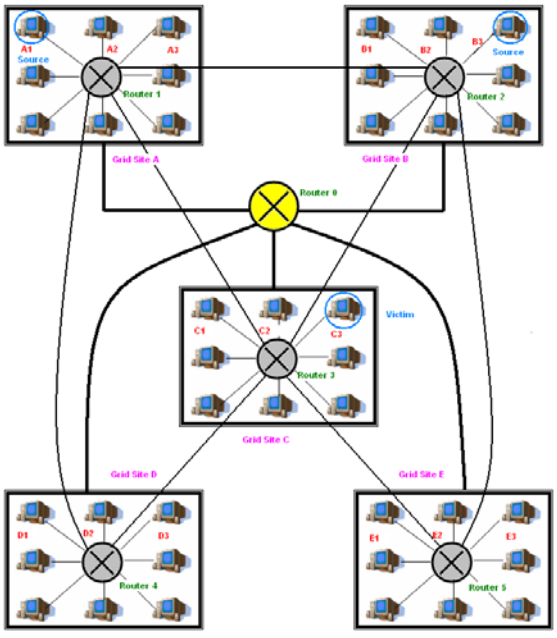

Fig. 12. Environment for statistical study

Consider Fig. 12, A1 and B3 are attack sources at different Grid Sites, while C3 is the target victim machine. Router 1 will capture traffic flow coming from A1 and Router 2 will capture attack flow thrown by B3, for a specified time window (w). Suppose that we capture the following traffic flow at Router 1 and Router 2, shown in table I and table II, table III and table IV respectively.

TABLE I: Traffic at Router 1

Source node	Destination node	No of packets	Entropy
A1	C3	7	0.50
A2	B1	2	0.40
A3	B3	3	0.47
A4	E1	2	0.40

Therefore Router Entropy for Router 1 is 0.50 + 0.40 + 0.47 + 0.40 = 1.77 & as $\log_2 4$ = log4/log2 = 2 Hence NE is 1.77/ $\log_2 4$ = 0.88

TABLE II: Traffic at Router 2

Source node	Destination node	No of packets	Entropy
B1	D1	2	0.44
B2	A3	1	0.31
B3	C3	6	0.47
B4	E2	2	0.44

Therefore Router Entropy for Router 2 is 0.44 + 0.31 + 0.47 + 0.44 = 1.66 & as log24 = log4/log2 = 2 Hence NE is 1.66/ log24 = 0.83

TABLE III: Traffic at Router 4

Source node	Destination node	No of packets	Entropy
D1	A1	2	0.46
D2	A3	2	0.46
D3	E3	3	0.52
D4	C2	3	0.52

Therefore Router Entropy for Router 1 is 0.46 + 0.46 + 0.52 + 0.52 = 1.96 & as $\log_2 4$ = log4/log2 = 2 Hence NE is 1.96/ $\log_2 4$ = 0.98

TABLE IV: Traffic at Router 5

Source node	Destination node	No of packets	Entropy
D1	C3	2	0.52
D2	C1	1	0.43
D3	D1	2	0.52
D4	A4	1	0.43

Therefore Router Entropy for Router 2 is 0.52 + 0.43 + 0.52 + 0.43 = 1.90 & as log24 = log4/log2 = 2 Hence NE is 1.90/ log24 = 0.95

We can see that as at both routers i.e. Router 1 and Router 2, routers entropy is lesser as only one flow conquered the whole bandwidth. As an outcome NE decreases. If we have a perfect threshold value δ, suppose 0.94 then our proposed ADS will consider flows coming from A1 (GS A) and B3 (GS B) as malicious flows, while Grid Site D & Grid Site E have entropy value greater than our considered threshold value 0.95, no attack is detected at these sites.

B. Simulations Study

1) Simulation Environment

GridSim was used as a simulation environment, for testing the results of our proposed Idea. To simulate our proposed idea we have 3 users with 2 posers of DDoS attack, 2 routers and 3 resources containing any single

victim node on the same time, as shown in Fig. 13.

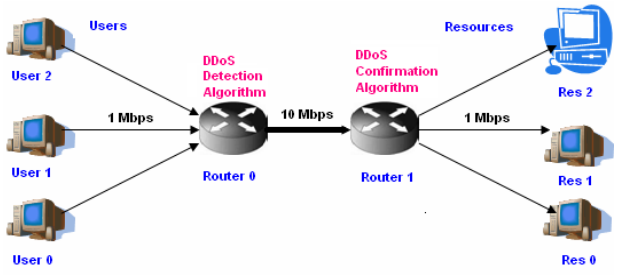

Fig. 13. Environment for simulation study

Both routers are connected to each other over a 10 Mbps link, while all other connections are made at 1 Mbps link. Detection algorithm is implemented on router 0, while confirmation is supposed to be implemented on router 1.

2) Simulation Results

In this section we consider only DDoS detection algorithm on router 0, not to confirm attack.

CASE 1:

TABLE V: TRAFFIC AT ROUTER FOR USER_0

Destination node	Total No of packets	Probability	Entropy
Res_0	5	0.5	0.5
Res_1	2	0.2	0.46
Res_2	3	0.3	0.52

Therefore Router Entropy for Router 2 is 0.5 + 0.46 + 0.52 = 1.48 & as log23 = log3/log2 = 1.58

Hence Normalized Entropy is 1.48/ $\log_2 3$ = 0.93

TABLE VI: TRAFFIC AT ROUTER FOR USER_1

Source node	Total No of packets	Probability	Entropy
Res_0	4	0.4	0.52
Res_1	3	0.3	0.52
Res_2	3	0.3	0.52

Therefore Router Entropy for Router 2 is 0.52 + 0.52 + 0.52 = 1.57 & as log23 = log3/log2 = 1.58

Hence Normalized Entropy is 1.57/ $\log_2 3$ = 0.99

TABLE VII: TRAFFIC AT ROUTER FOR USER_2

Source node	Total No of packets	Probability	Entropy
Res_0	0	0.0	0.0
Res_1	3	0.3	0.52
Res_2	7	0.7	0.36

Therefore Router Entropy for Router 2 is 0.0 + 0.52 + 0.36 = 0.88 & as log22 = log2/log2 = 1

Hence Normalized Entropy is 0.88/ $\log_2 2$ = 0.88

VII. PERFORMANCE EVALUATION

Our ADS can detect 100% DDoS attack only in case of good threshold value, which is one of the most challenging tasks in developing any ADS. We conclude our story that a threshold value of 0.95 results in good detection rate. A value greater than 0.95, results in good detection rate i.e. 100 % DDoS detection but generate more false positive alarms, as the value is increased from 0.95 to 1.0. The reports are shown in Fig. 14 and Fig. 15, are self explanatory.

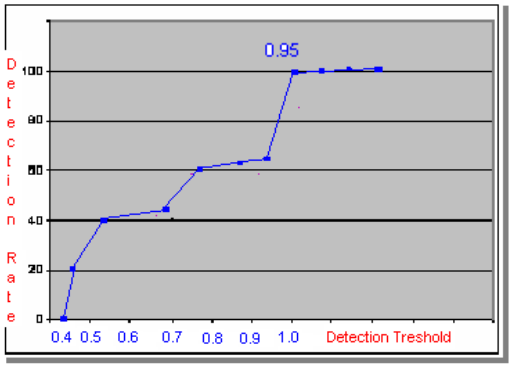

Fig. 14. DDoS detection rate

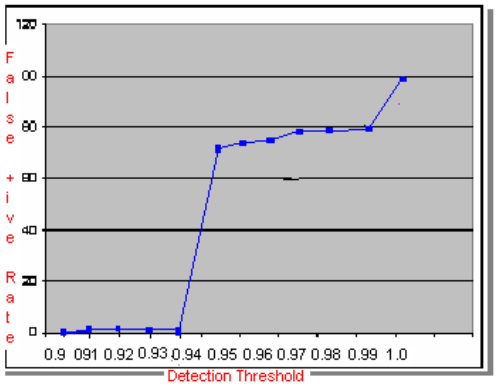

Fig. 15. DDoS false positive rate

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new architecture for Grid Computing platform. We have also developed ADS for detection & early prevention of DDoS attacks. In future the proposed idea may be actually implemented over Grid environment to accurately detect DDoS attacks. The idea may also be extended for recovery mechanism for DDoS attacks. Following are some challenges which might be addressed for further enhancement by researchers and scholars.

- Setting perfect threshold values δ_1, δ_2, some time it must be dynamic in nature to detect DDoS accurately
- what about different mathematical functions when used for creating attack packets
- In case of Huge network access separating legitimate flows from attack flows is a challenging task

REFERENCES

[1] B. Jacob, M. Brown, K. Fukui, and N. Trivedi, *Introduction to Grid Computing*, 2005.

[2] K. Samad, E. Ahmed, R. A. Shaikh, and A. A. Iqbal, *Analysis of DDos Attacks And Defense Mechanisms*, 2005.

[3] H. Chau, *Network Security – Mydoom, Doomjuice, Win32/Doomjuice Worms and DoS/DDoS Attacks*, USA.

[4] P. Zaroo, "A survey of DDoS attacks and some DDoS defence mechanisms," *Advanced Information Assurance* (CS 626).

[5] S. M. Specht and R. B. Lee, *Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures*, September 2004.

[6] Y. Chen, K. Hwang, and W. S. Ku, *Distributed Change Point Detection of DDoS Attacks: Experimental Results on DETER Testbed*, 2007.

[7] Preeti, Y. Chaba, and Y. Singh, *Review of Detection and Prevention Policies for Distributed Denial of Service Attack in MANET*, March 2008.
[8] S. Meenakshi and Dr. S. K. Srivatsa, *A Comprehensive Mechanism to Reduce the Detection Time of SYN Flooding Attack*, 2009.
[9] B. Parno, Z. Zhou and A. Perrig, *Don't Talk to Zombies: Mitigating DDoS Attacks via Attestation*, June 2009.
[10] K. Meintanis, B. Bedingfield and H. Kim, *The Detection & Defense of DDoS Attack*, University of Texas.
[11] A. Lakhina, M. Crovella, and C. Diot., "Diagnosing Network-Wide Traffic Anomalies," *ACM SIGCOMM Computer Communication Review*, Portland, 2004.
[12] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, *Statistical approaches to DDoS attack Detection and Response*, 2003.
[13] W. Lee and D. Xiang, "Information-theoretic measures for anomaly detection," IEEE, 2001
[14] D. Applebaum, *Probability And Information* (An Integrated Approach), Cambridge University Press, 2008.
[15] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Second Edition, 2006.
[16] D. A. L. Romaña and Y. Musashi, *Entropy Based Analysis of DNS Query Traffic in the Campus Network*, Japan.
[17] R. Buyya and M. Murshed, "GridSim: a toolkit for the modeling and simulation of distributed resource management and scheduling for Grid computing," 2002.
[18] A. Sulistio, G. Poduval, R. Buyya, and C. K. Tham, "Constructing A Grid Simulation with Differentiated Network Service using GridSim," University of Melbourne, Australia.
[19] M. Murshed and R. Buyya, "Using the GridSim Toolkit for Enabling Grid Computing Education," Monash University, Australia.
[20] A. Sulistio, U. Cibej, S. Venugopal, B. Robic, and R. Buyya, "A toolkit for modelling and simulating data Grids: an extension to GridSim," March 2008.
[21] A. Sulistio, C. S. Yeo, and R. Buyya, *Visual Modeler for Grid Modeling and Simulation (GridSim) Toolkit*, 2003.
[22] *Microsoft Encarta Encyclopedia*, 2009.
[23] C. E. Shannon, *A Mathematical Theory of Communication*, 1948.
[24] C. E. Shannon, *Communication Theory of Secrecy Systems*, 1949.
[25] Y. C. Wu, W. Yang, and R. H. Jan, *DDoS Detection and Trace-back with Decision Tree and Gray Relational Analysis*, National Chiao Tung University, Taiwan.
[26] G. Nychis, *An Empirical Evaluation of Entropy-based Anomaly Detection*, May 2007.

Muhammad Zakary is working as lecturer in computer science department of Abdul Wali Khan University Mardan, Pakistan. He is a new researcher to the field of new emerging computing technologies like Grid, Cloud and Green Computing. He has done MS in Computer Science and is interested for a doctorate degree in computer engineering. Currently he is working on security issues in Grid and Cloud computing i.e. distributed systems. He is interested in implementing Cloud computing over bioinformatics. He is also working and interested to Green the Cloud, Energy Efficient Scheduling for Real-Time Systems and Smarter Power Grids.

Muazzam Ali Khattak is working as lecturer in computer science department of Abdul Wali Khan University Mardan, Pakistan. He is a new researcher to the field of distributed systems. He is given a fully funded overseas PhD scholarship from Abdul Wali Khan University. Currently he is pursuing his PhD from Brunel International University, London. He is also interested in Green Computing. He is the author of several research articles in high performance computing and bioinformatics. His research topic is Smart Grid technology.