Volume 3, No. 1, Jan-Feb 2012

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Efficient Secure Techniques for Grid Based Peer-to-Peer Detection System

Rama Soni*
Department of C.S.E
Truba Engineering College
Bhopal, M.P, India
sonirajni.soni@gmail.com

Omkumari Soni
Lecturer of Information Technology
Dr. B. R. A. Polytechnic College
Gwalior, M.P., India
rajani_it@yahoo.com

Abstract- As distributed system architectures such as peer-to-peer, grid computing and MANET become more popular, there is an increasing need for robust and scalable mechanisms to establish trust between entities. The primary objective of Grid computing is to support the sharing of resources and service spanning across multiple administrative domains. Due to the inherently dynamic and multi organizational nature maintaining security of both users and resources is the challenging aspect of Grid. Grid uses internet as an infrastructure to build communication, with the fusion of web services and grid technologies further increases the security concerns for their complex nature. This paper takes a look at the vulnerability of Grid environment on denial of service attack. We found that deploying an efficient intrusion detection system to Grid can significantly improve its security and it can detect denial of service attack before it affects the victim. But due to the special characteristics and requirement of Grids, the existing traditional intrusion detection system cannot work properly in that environment. The focus of this paper is to investigate and design an anomaly detection system which can detect DoS and DDoS attack with high attack detection and low false alarm rate to achieve high performance. We have extensively surveyed the current literatures in this area; the main stress is put on feature selection for the Grid based anomaly detection system. An entropy based anomaly detection system has been proposed; also we have discussed the advantage of taking entropy as the metric. Finally the performance of the system has been analyzed using NS2 network simulator.

Keywords- MANET, Grid Computing, Anomaly Detection Technique.

I. INTRODUCTION

The name 'Grid' comes from analogy with the Electricity Grid. Users can obtain a resource such as electricity, or in this case computer processing from a variety of sources to supply their needs. The goal is to provide users with access to the resources they need and when they need them. Initially Grid systems were developed for supporting scientific computations. Today, many enterprises and researchers are looking to use the Grid approach to commercial uses and for applications in many different areas. Security in Grid systems however has not been much addressed and yet is an important issue to make it usable in a variety of commercial application [1] and [2].

In Grid environments, where the computational, storage, and network resources are inherently heterogeneous, dynamic and multi organizational in nature, the issue of managing security of both resources and users are most challenging. Although Grid Security Infrastructure (GSI) of grid middleware provides several security features that required on grid environment; include X.509 certificates, authentication algorithm using Secure Socket Layer (SSL) protocol, authorization, delegation, auditing and single sign. An intruder can explore security flaws in any of the other components like operating system (OS), network protocols and non grid application running in the same environment. Moreover grid cannot defend itself against stolen passwords and legitimated users who abuse their privileges to execute malicious activities and due to the huge resource capacity like computational and storage, grid may become a next platform for the attackers. If an intruder got unauthorized access to grid, the grid resources can misused in different ways; like the huge computational power can be used for breaking passwords or security systems , the large storage capacity can be used to store illegal software , data and the huge bandwidth can be used for lunching Distributed Denial of Service (DDoS) attack. Possible security threats associated in grid, out of which Denial of Service attack (DoS) and Distributed Denial of Service attacks (DDoS) are the most common and deadly attack today.

Intrusion detection system (IDS) are widely used for detection of Denial of Service attack in a network or within a system and it can be deployed in grid to complement existing measures like authentication, authorization, access control [3] and [4].

Along with those basic security measures Grid-specific Intrusion Detection System is capable of functioning in a real-life grid environment, which has the potential to detect before Denial of Service attack succeeds. The purpose of this research is to designing an anomaly detection system for detecting real-life grid misuse. To secure grid from DoS attack its must be detected before it affects the end user with high detection rate and low false alarm rate, So that attack traffic will be discarded, without affecting legitimate traffic. In case of DDoS attack, the attack packets comes from ten or thousand of sources and DoS defense system that is based upon monitoring the volume of packets coming from a single address or single network will fail since the attack comes from various sources. Intrusion detection systems are widely used for DDoS attack detection.

An intrusion detection system (IDS) inspects all inbound and outbound network and system activity and identifies possible security threats in a network or in a system. IDSs can be classified, based on their functionality, as misuse detectors and anomaly detectors. Anomaly detection has an advantage over signature-based is that a new attack can be detected if it falls out of the normal traffic patterns. Due to the special characteristics and requirement of computational grids, detecting such difference in traffic patterns imposed some new unique challenges that did not exist in traditional intrusion detection system. One of the properties of Grid Security Infrastructure (GSI) is the confidentiality of the

data transferred over the network. For which the data transmitted over the grid must be encrypted and the system could not see the data payload portion of the packet because of encryption. Analysis would be based only on the low level information, which can be extracted from the packet header. The Next problem is to find a metric that can extract distribution of traffic features that can be used in anomaly detection system.

II. BACKGROUND

A. Grid Computing:

The basic idea of grid computing is to provide an infrastructure for solving massive computational problems by using the idle resources (CPU cycles, disk storage, and network bandwidth) of large number of computers, servers embedded in a distributed infrastructure. The aim is getting computers to work together for solving a particular problem. In every organization, there are large amounts of underutilized computing resources. According to IBM survey Mainframes are idle 40% of the time, UNIX servers are actually "serving" something less than 10% of the time and most desktop machines are busy less than 5 percent of the time.

Grid computing provides a framework for exploiting these underutilized resources to solve problems which are beyond the scope of single processor and also increases the efficiency of resource usage. In addition to scientific experiment, industries such as bio-medical field, modeling, oil exploration, motion picture animation, weather prediction and many others needs massive computing power. In grid environment a single large job can be split into smaller pieces and run on several computers simultaneously which is too intensive for any stand alone machine [3].

B. Types of grids-

Grid computing can be used in a variety of ways to address various kinds of application requirements. Often, grids are categorized by the type of solutions that they provide. The three primary types of grids are summarized below.

C. Computational grid:

A computational grid provides secure access to huge pool of shared processing power suitable for high throughput applications and computation intensive computing. It focused on specifically for computing power. Computational Grid also called Meta computer.

D. Data grid:

Data grids provide an infrastructure to support data storage, data discovery, data handling, data publication, and data manipulation of large volumes of data stored in heterogeneous databases and file systems across multiple organizations. Different datasets stored in different locations create an illusion of mass storage. These are often, but not always, combined with computational grid systems.

E. Service grid:

In service grid unused resources are exported to the users in the form of service. It creates a "grid" from the unused resources in a network of participants. With the evolve of open grid architecture (OGSA), open and standard protocols it provides services and supports dynamic creating, running, maintaining and cancellation of application. The QOS is an important parameter for a service grid system to meet the user demand [2] and [5].

F. Grid components-

Grid basically contains five Components.

i. A portal
ii. A service broker
iii. Task scheduler
iv. A task manager
v. A group of grid node.

a. ***The portal*** acts as a user interface, through which user can log in and use the grid. After having logged into the grid, a user can submit a task.

b. ***The service broker*** identifies the list of resources for handling a particular task submitted by the user and selects the optimal one which is available now.

c. ***A scheduler*** sets rules and priorities for scheduling jobs on a grid-based infrastructure. It is responsible for scheduling submitted tasks.

d. ***The task manager*** finally launches a submitted task.

e. ***The nodes*** can be desktops, servers, Workstations and clusters that belong to different LANs, WANs, or the Internet.

G. Grid Security:

Generally first generation grid was deployed across mutually trusting administrative domains like research laboratories, academic institutions and for military use, But OGSA (Open Grid Services Architecture) [5] as a standard for interoperable next-generation grids, many commercial enterprises are beginning to use grid technologies as well.

As grid is being used commercially, maintaining the QoS, level of security demand by users and resource security, resource integrity, confidentiality of communication, privacy of user information are prime concerns. Grid security itself imposes several unique security challenges, including managing user identities across local and global networks, trust relationships between entities, end-user key and credential management, and providing security to resources against malicious acts from grid users. The fusion of web services and grid technologies further increases the concerns about security problem for their complex nature. Security is a very important component of the Grid, as misuse of its vast resources can result in considerate damage [6].

H. Security Threats classification in Grid:

Although grid security system provides fundamental security mechanisms like authentication, authorization, confidentiality also web services provides security systems like WS-security, WS-conversations, still there are many other possible security threats associated with grid environment.

I. User Threats:

When user credentials are not secure enough or the fundamental security mechanism like authentication or authorization are not carried out properly, there is a chance that different user threats will generate.

J. Mediator Threats:

During the communication between user and service or resource provider, mediator carries the corresponding data or message in XML format. So mediator threat consists of those threats originating from insecure service level communication. Insecure communication includes eavesdropping and intercepting service communication.

K. Service Provider Attack:

The service provider takes the job submitted by the user, process them and send back the result to the user with quality-of-service. So service threats are those kinds of threats that composed of malicious input to get malicious goal like malicious code/ malware.

L. Resource Provider Attack:

A resource provider provides supplies two types of resources including physical resources like CPU cycles, storage, bandwidth etc and software resources. So resource provider threats composed of those kinds of threats that are unauthorized use of the physical resources or integrity threats or destroying the software resources [6] and [8].

M. Related Work:

Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) are the most dreadful network threats in recent years. The vulnerabilities of grid environment in the presence of DDoS have been presented and they have proposed a distributed defense system for grid. In recent, authors discussed the need for an intrusion detection system in grid environment. They have classified grid intrusions in to 4 types i.e. 1) Unauthorized access 2) Misuse 3) Grid exploit 4) Host or Network-specific attacks. They proposed a model that is composed of high-level GIDS (Grid intrusion detection system) that utilizes functionality of lower-level HIDS (Host intrusion detection system) and NIDS (Network intrusion detection system) provided through standard inter-IDS communication. Different techniques and challenges involved in anomaly detection system can be found. Many articles use traffic volume [flow, packet, byte count] as the metric for anomaly detection system. Volume based detection scheme were proved as a good metrics for anomaly detection system and it can detect anomalies that causes large traffic changes , but small DoS attacks that do not cause much changes in traffic cannot be detected perfectly.

The attack discussed above can be better detected by analyzing distribution of traffic features. A traffic feature is a field in the header of the packet. One of the properties of Grid Security Infrastructure (GSI) is confidentiality of the data transferred over the network. For which the data transmitted over the grid must be encrypted. So the system could not see the data payload portion of the packet because of encryption. Analysis would be based only on the low level information, which can be extracted from the packet header. The Next problem is to find a metric that can extract distribution of traffic features that can be used in anomaly detection system. Recently there has been use of entropy and traffic distribution for detecting DDoS attack anomalies.

A number of articles suggested entropy as a metrics to summarizing traffic distribution for anomaly detection. In previous author uses entropy of distribution of source (destination) address for DDoS detection. included PCA framework with entropy based metrics and shown that it can detect wide variety of types of anomalies that cannot identified using volume based analysis only. Lee and Xiang suggested use of different information theoretic measures for detecting malicious activities. Recently authors use entropy rate to discriminate the DDoS attack from legitimate traffic. The use of entropy for analyze changes in traffic distribution has two benefit. i) Using entropy for anomaly detection increases the detection capability than volume based methods. ii) It provides additional information to classify among different types anomaly (worms, DoS attack Port scanning) [7] and [9] and [10].

We considers two classes of distribution i) flow header features (IP address, ports, and flow sizes) ii) behavioral features (the number of distinct destination / source address that a host communicates with). The anomaly detection system discussed in this paper is based on by analyzing the change in entropy of above two traffic distributions. Our objective in this paper is to design an anomaly detection system based on entropy and entropy rate to detect DDoS attack in grid environment. We use normalized entropy which calculates the over all probability distribution in the captured flow in our algorithm to get more accurate result.

III. PROPOSED TECHNIQUES

A. Proposed an Anomaly Detection Scheme:

Entropy or Shannon-Wiener index is an important concept of information theory, which is a measure of the uncertainty or randomness associated with a random variable or in this case data coming over the network. The more random it is, the more entropy it contains. The value of sample entropy lies in range [0, logn]. The entropy value is smaller when the class distribution is pure i.e. belongs to one class. The entropy value is larger when the class distribution is impure i.e. class distribution is more even. Hence comparing the value of entropy of some sample of packet header fields to that of another sample of packet header fields provides a mechanism for detecting changes in the randomness.

The entropy H (X) of a random variable X with possible values {x1, x2…, xn} and distribution of probabilities P = {p1, p2, . . . , pn} with n elements, where 0 ≤ pi ≤ 1 and = 1 can be calculated as:

$$\sum_i \text{pi}$$

$$H(X) = -\sum_{i=1}^{n} \text{p(xi)} + \log \text{P(xi)} \qquad \text{……..(1)}$$

In our proposed anomaly detection algorithm we use entropy as a principal matrix. We use change of entropy of traffic distributions (IP address, port) for DDoS detection. If we are interested in measuring the entropy of packets over unique source or destination address then maximum value of n is 232 for ipv4 address. If we want to calculate entropy over various applications port then n is the maximum number of ports. Here p (xi) where xi Î X is the probability that X takes the value xi. Suppose we randomly observe X for a fixed time window w, then p (xi) = mi/m, where mi is the frequency or number of times we observe X taking the value xi i.e.

$$m = \sum_{i=0}^{n} \text{mi}$$

$$H(X) = -\sum_{i=0}^{n} (\text{mi} \qquad \text{/m)+(log }_i\text{/m)……..(2)}$$

If we want calculate probability of any source (destination) address then, mi = number of packets with xi as source (Destination) address and m = total number of packets

$$P(Xi) = \frac{\text{Number of packets with xi as source (destination) address}}{\text{Total number of packets}}$$

Here total number of packets is the number of packets seen for a time window *T*. Similarly we can calculate probability for each source (destination) port as

$$P(Xi) = \frac{\text{Number of packets with xi as source (destination) port}}{\text{Total number of packets}}$$

Normalized entropy calculates the over all probability distribution in the captured flow for the time window *T*.

Normalized entropy = (H / log n0) ……(3)

Here n0 is the number of distinct xi values in the given time window. In a DDoS attack from the captured traffic in time window *T*, the attack flow dominates the whole traffic, as a result the normalized entropy of the traffic decreased in a detectable manner. But it is also possible in a case of massive legitimate network accessing. To confirm the attack we have to again calculate the entropy rate. Here flow is packages which share the same destination address/port. In this mechanism we have taken one assumption that the attacker uses same function to generate attack packets. According to a stochastic processes the entropy rate H (c) of two random processes are same.

H (c)= …(4)

$$\lim_{n\to\infty} \frac{1}{n} H(x1, x2, \ldots xn)$$

The steps in our proposed DDoS detection algorithm are described in figure:

Step i: Collect sample flows for a time window *T* on the edge routers.

Step ii: Calculate router entropy $H(X) = -\sum_{i=1}^{n} p(xi) + \log P(xi)$

Step iii: Calculate NE = (H / log n0) where, NE = normalized router entropy.

Step iv: If NE < threshold (δ1), identify the suspected attack flow.

Step v: Calculate the entropy rate H (c)= $\lim_{n\to\infty} \frac{1}{n} H(x1, x2, \ldots xn)$ of the suspected flow in that router and the routers on downstream.

Step vi: Compare Hi (c) "ie entropy rates on routers.

Step vii: If Hi (c) £ threshold (δ2), it is a DDoS attack. Else legitimate traffics.

Step viii: Discard the attack flow.

Figure 1: DDoS detection algorithm

Definition 1:

A stochastic process {X (t), t Î T} is a collection of collection of random variables. For each t Î T, X (t) is a random variable. We refer X (t) as the state of the process at time t. The set T is called the index set of process.

Definition 2:

A stochastic process is said to be stationary if the joint distribution of any subset of random variables is invariant with respect to shifts in the time index i.e.

Pr{X1 = x1, X2 = x2. . . Xn = xn}= Pr{X1+l = x1, X2+l = x2. . . Xn+l = xn}

Definition 3:

The entropy rate is the rate of growth of entropy of a random process. If we have a sequence of n random variables, then the entropy rate of a stochastic process { xi } is defined by

H (c)=

$$\lim_{n\to\infty} \frac{1}{n} H(x1, x2, \ldots xn)$$

B. Implementation Details-

Using figure 2 how the proposed anomaly detection system can be implemented in grid infrastructure and how routers will communicate with each other to detect the attack. Grid computing can be thought as a virtual organization which is a collection of some real organizations or sites. In the figure 2 we have shown a grid topology model which is a collection of four sites i.e. site A, site B, site C and site D and they are connected by 5 routers. We employ our proposed anomaly detection system in each router of the grid infrastructure. Edge routers near the source of traffic will capture flows for a predefined time window *T* and calculate the router entropy and normalized router entropy. If the normalized router entropy is less than certain threshold δ1 identify the suspected DDoS attack flow from the traffic. But it is also possible in a case of massive legitimate network accessing. To confirm the attack the entropy rate of the suspected flow is calculated in that router according To "Eq. (4)".

Based on the destination address on the IP header of the packets and routing table it discovers the downstream routers and sends security alarm to those routers to calculate entropy rate of the suspected flow. As discussed above, the entropy rates of attack flows at different routers in the network are same. If the calculated entropy rates on routers are same or very near, the attack is confirmed. We have taken two examples using figure 2 how the detection scheme works.

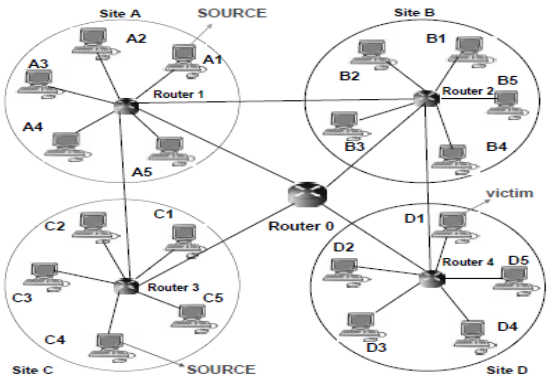

Figure 2: Grid Topology

Suppose node A1 and C4 are attack sources and D1 is the victim. Based on the DDoS detection algorithm flows coming A1 will first captured by router 1 and flows coming from C4 will be captured by router 3. Suppose at router 1, router 3 and router 2 we have captured flows as given in table 2, table 3 and in table 4 respectively in a fixed time window *T*. The router entropy is calculated according to "Eq. (2)"and the normalized router entropy is being calculated using "Eq. (3)".

Although the data are taken manually we can see that for router 1 and router 3 the normalized router entropy is comparatively less than the router 2. In the first two cases one flow dominates the whole traffic as a result the normalized entropy decreases. After which the entropy rate is being calculated. In figure 2, for router 1 the entropy rate

of suspected flow is calculated and compared in router1 and router 0. Similarly for router 3 the entropy rate of those flows will be calculated and compared both in router 3 and router 0. While the entropy rates of different routers are same or less than δ2, the attack is confirmed and attack flow is discarded. All the above calculations are based on log2.

IV. EXPERIMENTAL RESULTS

The simulation was done using NS-2 simulator to evaluate the performance of our DDoS detection algorithm with results from the experiment. Our simulation includes 3 source, 2 intermediate routers and 2 destination nodes as shown in figure 3. Out of which 3 source nodes 2 nodes are attackers and 1 node is a legitimate user. The bandwidth of legitimate traffic is set constant and the simulation of attack traffic is achieved by randomly generating many pairs of Constant Bit Rate (CBR) UDP flows in NS2. The legitimate user to send packets from the time of .20 second and the attacker starts sending attack traffic at .30 seconds. The experiment lasts at 3 second. We traced no of packets received in every 0.5 second interval.

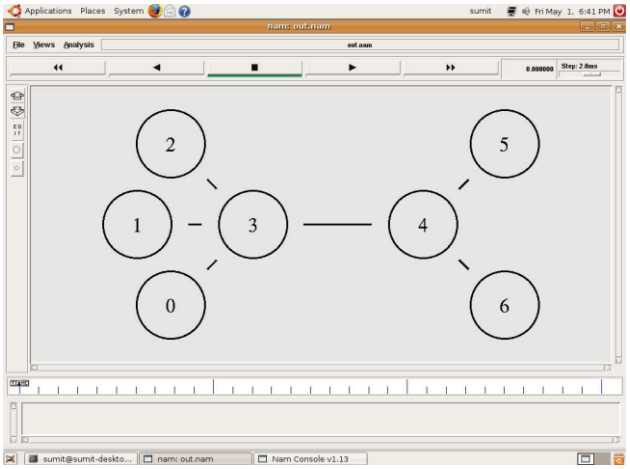

Figure 3: Screen shot of Setup

We consider 2 situations in our simulation to evaluate the performance of our proposed algorithm. In the first situation, we start the attack without using any defense mechanism and study how the system performance is being degraded. In this case the router at the victim simply drops packets including legitimate packets which it cannot handle. In the second situation, we deploy the entropy based anomaly detection system in the simulation network and examine how the system performance increases significantly. The graph in Figure 4 depicts the effect of DDoS attack without any defense system. It shows numbers of attack packets as well as legitimate packets with respect to time. We can mark that within same time different zombies combined to send attack packets as a result the number of attack packets increases significantly. For which the packet drop rate of legitimate users increases dramatically as shown in the Figure 5.

We use 2 metrics attack detection rate and false-positive rate as performance evaluation metrics.

a) Detection Rate Rd = d / n

d = number of attack packet detected in the simulation experiments.

n = total number of attack packet generated.

The figure 6 shows attack detection rate of our proposed algorithm with respect to detection threshold. We found that the attack detection rate detection is almost 100% when the detection threshold δ1 i.e normalized entropy is more than 0.92. But after calculating the false positive rate we will finalize the threshold δ1 in this experiment.

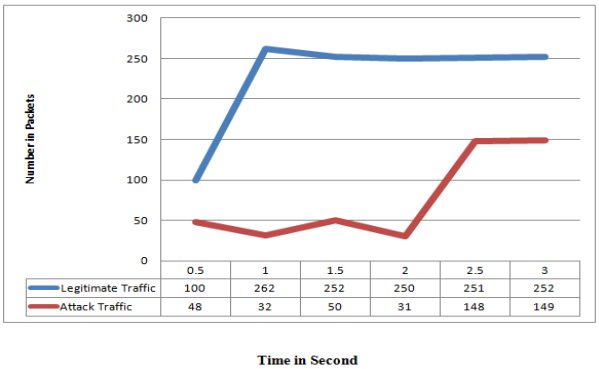

Figure 4: Effect of DDoS Attack

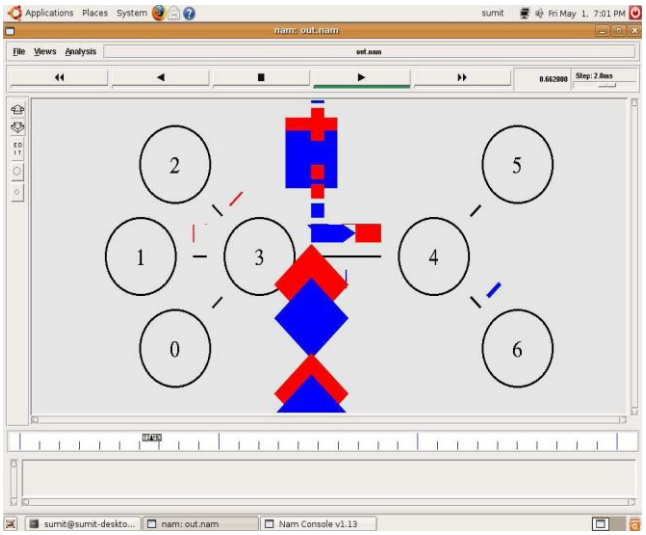

Figure 5: Screen shot of packet drop

b) False positive Rate Rfp = p / m

P = number of false positive raised

m = number of legitimate traffic flow checked by the simulator

When calculating false positive rate we found that up to setting detection threshold 0.94 the false positive rate is 0, but putting threshold 0.95-0.99 increases false positive rate 67.26 and after then false positive rate 100%.

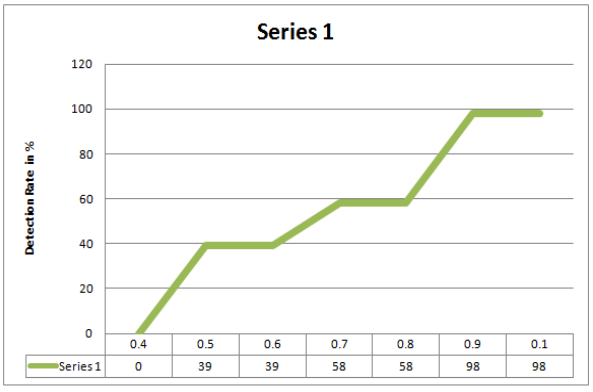

Figure 6: DDoS attack Detection Rate

According to the obtained simulation results, if we will take the detection threshold δ1 as 0.94 then, the proposed anomaly detection system can detect DDoS attack traffics with 100% detection rate and without any false positive. If the normalized router entropy in any case will be less than 0.94 it starts detecting the suspected flow. Again entropy rate is being calculated according to the DDoS detection algorithm 2 to confirm the attack.

V. CONCLUSION

This paper takes a look at different vulnerability associated with grid. Out of which Distributed Denial of Service is an immense thereat to grid services. We found that applying IDS to it can significantly increase its security which can deploy along with existing security measures. But existing IDSs are not designed to be grid specific. The objective of this study was to investigate how DDoS attack affects the grid performance and designing a grid specific anomaly detection system. DDoS attack is a major threat that cannot be addressed well if various defense systems do not organize in to framework exchanging information and services.

The attack must be detected and blocked before reaching the victim and with high detection rate and low false alarm rate. In this paper we have used information theoretic parameters entropy and entropy rate to model the anomaly detection system for grid. We have implemented anomaly detection system in each router of the grid environment and the router will cooperate with each other to detect anomaly. The main advantage of the above proposed method is the attack is detected and blocked before reaching the victim and with high detection rate. But the challenge lies in this approach if the attacker will use different packet generation functions in an attack and setting a good threshold. As a next step we are going to work to eliminate the attacker uses same attack generation function to create attack packets at compromise hosts or zombies, but if attacker starts generating attack packets using different attack packet generation function and also setting up a good threshold Value is very difficult and that should be dynamic depending up on the current situation.

VI. REFERENCES

[1]. Amy Poh Ai Ling and Mukaidono Masao, "GRID INFORMATION SECURITY FUNCTIONAL REQUIREMENT", International Journal of Grid Computing & Applications (IJGCA) Vol.2, No.2, June 2011, pp 1-19.

[2]. Mohammed Bakri Bashir, Muhammad Shafie Bin Abd Latiff, Aboamama Atahar Ahmed, Yahaya Coulibaly , Abdul Hanan Abdullah and Adil Yousif, "A HYBRID RESOURCE DISCOVERY MODEL FOR GRID COMPUTING", International Journal of Grid Computing & Applications (IJGCA) Vol.2, No.3, September 2011, pp 1-12.

[3]. Adil Yousif, Abdul Hanan Abdullah, Muhammad Shafie Abd Latiff and Mohammed Bakri Bashir, "A Taxonomy of Grid Resource Selection Mechanisms", International Journal of Grid and Distributed Computing Vol. 4, No. 3, September, 2011, pp 107-117.

[4]. Krishnadas N, "Designing a Grid Computing Architecture: A Case Study of Green Computing Implementation Using SAS", SAS Global Forum 2011.

[5]. C.Valliyammai, S.ThamaraiSelvi, R.Satheesh Kumar, E.Pradeep, and Naveen.K, "AN ALTERNATE APPROACH TO RESOURCE ALLOCATION STRATEGY USING NETWORK METRICSIN GRID", International Journal of Grid Computing & Applications (IJGCA) Vol.1, No.2, December 2010, pp 27-37.

[6]. Leyli Mohammad Khanli, Maryam Etminan Far and Ali Ghaffari, " Reliable Job Scheduler using RFOH in Grid Computing", Journal of Emerging Trends in Computing and Information Sciences, VOL. 1, NO. 1, JULY 2010 ISSN 2079-8407, pp 43-47.

[7]. Peter Crossley, Agnes Beviz, (2010) "Smart energy systems: Transitioning renewables onto the grid", Renewable Energy Focus, Volume 11, Issue 5, September-October, pp. 54-56, 58-59.

[8]. James Heidell, Harold Ware, (2010) "Is There a Case for Broadband Utility Communications Networks? Valuing and Pricing Incremental Communications Capacity on Electric Utility Smart Grid Networks", The Electricity Journal, Volume 23, Issue 1, January-February, pp. 21-33.

[9]. Pertti Järventausta, Sami Repo, Antti Rautiainen, Jarmo Partanen, (2010) "Smart grid power system control in distributed generation environment", Annual Reviews in Control, Volume 34, Issue 2, December, pp. 277-286

[10]. G. Laccetti, G. Schmid, (2007) "A framework model for grid security", Future Generation Computer Systems, Volume 23, Issue 5, June 2007, pp.702-713.

