Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network

[1] Mueen Uddin, [2] Raed Alsaqour, [3] Maha Abdelhaq

[1] *Faculty of Computing and Technology, Asia Pacific University of Technology & Innovation*
Bukit Jalil, 57000*, Kuala Lumpur, Malaysia*
[2, 3] *School of Computer Science, Faculty of Information Science and Technology*
University Kebangsaan Malaysia, Bangi, 43600*, Selangor, Malaysia*
[1] Mueenmalik9516@gmail.com, [2] raed@ftsm.ukm.my, maha.ukm@gmail.com

Abstract

Background/Objectives

Distributed Denial of Service (DDoS) attacks are an increasing threat to the Internet community. Intrusion Detection Systems (IDSs) have become a key component in ensuring the safety of systems and networks. As networks grow in size and speed, efficient scalable techniques should be available for IDSs. Gnutella is a Peer to-Peer (P2P) networking model that currently provides decentralized file-sharing capabilities to its users but the distinction between server and client is pale. Due to Gnutella's dependence on a central unit, the program is vulnerable to security breaches. Methods/Statistical analysis: An IDS to detect DDoS attacks by simulating Artificial Immune System (AIS) is herein proposed. The proposed system uses an algorithm based on anomaly and signature-based detection mapped to AIS called "Generation of Detector (Genetic Algorithm)" to detect DDoS attacks. Each time an attack is identified, a new generation is added to the detectors dataset to detect the intrusions. Results: **S**imulation results show that the proposed method not only has adaptability, scalability, flexibility and variety but also has high accuracy and correctness. Conclusion/Application: The proposed algorithm efficiently reduces the false positives, thus the detection rate of intrusions is increased. Hence, the overall detection rate increases which ultimately increases the functional efficiency of the network to an acceptable level.

Keywords: Arti icial immune system, DDoS attack, Gnutella hybrid P2P network, Genetic Algorithm, Intrusion Detection System.

1. Introduction

Internet community is trying to cope with the series of DDoS attacks that shut down some of the world's most high profile and frequently visited Web sites. The whole phenomenon of communication process signifies the importance of reliable and unfailing trustworthy transportation of data and information from source to destination. In this concern of intact data transportation, much development of protocols and their improvements yield very progressive results providing efficient transmission and reception of complete and undamaged data. Current Information Technology (IT) trends are operating to provide easy and simple measures envisioned for reliable, efficient and error free communication (Uddin *et al.*, 2012). Traditional network file systems provide reliable way for users on a Local Area Network (LAN) to pool and share data. Internet-wide file sharing is still in its infancy. Software developers and researchers are struggling to find new ways to reliably, efficiently and securely share data across wide area networks that are plagued by high latency, bottleneck and unreliable or malicious nodes (Uddin & Rahman, 2011).

However, the current status of P2P networks is not well known due to their dynamic behavior because of churn; peers are continually joining and leaving the network in even a short period. P2P network infrastructures have made an enormous impact on the Internet, directly affecting its performance and security. These networks have grown rapidly to provide a platform for different users. Current applications of P2P network like Gnutella (Greensmith *et al.*, 2006),(Gnutella website. http://www.gnutella.com) and Morpheus (Johnson *et al.*, 2001)2001 provide a platform for file sharing, and an infrastructure for developing different applications to support network traffic (Andrade *et al.*, 2007), (I. Foster *et al.*, 2001), (Wang *et al.*, 2005), (Hwang *et al.*, 2006). The emergence of semantic web and semantic web services (Berners-Lee *et al.*, 2001), (McIlraith *et al.*, 2001) has opened the ways for many researchers and industry developers to use these protocols in P2P networks to enhance the scalability of networks. These networks are characterized by self-organization, symmetric communication and distributed control by automatically rearranging itself to joining and leaving nodes (Rousso-poulos *et al.*, 2004).. P2P network dynamic behavior has a huge impact on the performance of network. However, this behavior is not well known because there is no management system available to handle it and at the same time network size is large enough to be handled properly and smoothly to run the network services and applications appropriately.. These networks take advantage

of existing computing power, computer storage and networking connectivity, allowing users to leverage some of the major applications of P2P networks like file sharing, distributed computation, Ad hoc networks and collaborative applications.

Gnutella is decentralized P2P file-sharing protocols used to share, store, and retrieve and download any type of files across network (Gomes, 2001). It defines the way in which servents communicate over the network. It consists of a set of descriptors used for communicating data between servents and set of rules governing the inter-servent exchange of descriptors. Due to its distributed nature, network of servents that implements Gnutella protocol is highly fault-tolerant, as operation of the network will not be interrupted if a subset of servents goes offline (Roddy, 1989). Recent advances in P2P networks have resulted in hybrid architectures, represented by the success of Gnutella protocol 0.6 (Hatsuda & Motozumi, 1998)IEEE Transactions on</secondary-title></titles><periodical><full-title>Aerospace and Electronic Systems, IEEE Transactions on</full-title></periodical><pages>23-32</pages><volume>34</volume><number>1</number><dates><year>1998</year></dates><isbn>0018-9251</isbn><urls></urls></record></Cite></EndNote> and Kazaa (Panagopoulos *et al.*, 2004)2004. Gnutella was designed to meet the following goals: First, ability to operate in a dynamic environment, where hosts may join or leave the network frequently. They must achieve flexibility to keep operating transparently despite a constantly changing set of resources. Second, performance and scalability**,** the value of a network to an individual user scales with the total number of participants. As increasing the number of nodes, aggregate storage space and file availability should grow linearly, response time should remain constant, while search throughput should remain high or grow (Katz & Shapiro, 1994). Third, reliability, where external attacks should not cause significant data or performance loss. Finally, anonymity, which is valued as a means of protecting the privacy of people seeking or providing unpopular information.

Gnutella protocol 0.6 employs a hybrid architecture combining centralized and decentralized model (Hwang, et al., 2006). Servents are categorized into leaf and ultrapeer. A leaf keeps only a small number of connections to ultrapeers. An ultrapeer maintains connections with other ultrapeers and acts as a proxy to the Gnutella network for the leaves connected to it. An ultrapeer only forwards a query to a leaf if it believes the leaf can answer it, and leaves never relay queries between ultrapeers. Both of these versions are compatible with each other.

The proposed algorithm, implemented in this paper, is to detect DDoS attacks is mainly based on Gnutella protocol, used for P2P communication in Gnutella decentralized file-sharing system on Internet. There were other protocols for file sharing but main reason for choosing Gnutella protocol is the simplicity and scalability of its communication model and also very suitable for evaluating network performance. Furthermore, it is regarded as being able to adapt very well to dynamically changing peer populations (Oliveira *et al.*, 2005).

1.1 Security/performance issues in Gnutella Networks

The possibilities of attacks are enormous in P2P networks. Some of most common attacks (Roddy, 1989) are: Rational , File poisoning, Sybil , Eclipse and Distributed Denial of Service (DDoS) attacks. Gnutella is relatively simple protocol and does not embed any security features. As a consequence, it is prone to a number of vulnerabilities, threats and performance flaws. Traffic in Gnutella hybrid P2P network can be examined from different aspects like, the distribution of packet entrance in time unit, the interval between packet entrance and the distribution of packet size. If the number of packets exceeds the threshold value, the network resources become saturated, because the nodes (servents) leave or join the network at any time (Roddy, 1989), (M. Foster & Ripeanu, 2002), (Beverly Yang & Garcia-Molina, 2003). As a result, node will be exposed to DDoS attacks and such behaviors should be detected and prevented. In order to prevent, detect, encounter and stop these attacks, security should be recognized and formed over the network (G.Oikonomou *et al.*, 2006). Some of the noticeable factors in vulnerability of Gnutella hybrid P2P network are the flooding created when multiple messages (packets) are sent at the same time over the network without knowing the exact destinations and the decentralized nature of the Gnutella network (Li Xiao *et al.*, 2005).

Some of the other security threats very common to most P2P systems, for instance, IP address harvesting and privacy violation through traceability of peers (Exploiting the security weaknesses of the gnutella protocol. http://www.cs.ucr.edu/ csyiazti/courses/ cs260-2/project/gnutella.pdf.), (Broch *et al.*, 1998)1998, (Das *et al.*, 2000)2000. Traditional ways to hide IP addresses, such as proxies or bouncers, are not viable for large-scale massive file transfers. In a P2P network, any file transfer implies establishing a direct connection between nodes and consequently the possibility of tracing IP addresses, scanning hosts and knowing at least part of the shared files of other peers. Several papers have examined such threats, but none have proposed a practical solution. However, such studies have shown that the widespread assumption that a fully decentralized system like Gnutella protects users' privacy, more than a hybrid, is wrong (Broch, et al., 1998). In fact, centralized directories represent a higher risk than pure P2P only for the owners of the system, who can be easily traced by authorities and held responsible for the whole P2P system. Leaf users can be equally traced and sued for sharing illegal content in any type of P2P system, unless the single users adopts some preventive measures, e.g. blacklists (Broch, et al., 1998).

A Denial of Service (DoS) attack is an attack on a computer or a network that causes the loss of a service (Roddy, 1989). Many methods exist to perpetrate DoS attacks. In the case of P2P

networks, the most common form of a DoS attack is an attempt to flood the network with bogus packets, thereby preventing legitimate network traffic. Another method is to drown the victim in fastidious computation so that it becomes too busy to answer other queries. DoS attacks are far more efficient if multiple hosts are involved in the attack, we then speak of a DDoS attack (Chang, 2002), (Dubendorfer & Wagner, 2003). In a DDoS attack, the attacking computers are often personal computers with broadband connections that have been compromised by viruses or Trojans. The perpetrator can then remotely control these machines (qualified as zombies or slaves) and direct an attack at any host or network. Finally, a DDoS attack can be even further amplified by using uncompromised hosts as amplifiers. The zombies are answering packets to the victim. This is known as reflection attack (Dubendorfer & Wagner, 2003). As DDoS attack contains large number of distributed machines, the development of defensive nodes would be effective in discovering DDoS attack (G.Oikonomou, et al., 2006), (Mirkovic *et al.*, 2003). DDoS attacks take advantage of the hosts on the Internet with poor security. The perpetrators breaks into such hosts, install slave programs, and at the right time instruct thousands of these slave programs to attack a particular target. Since this attack does not exploit a security problem at the target, no mechanism currently exists to defend against such an attack. Collaborative discovery requires that heterogeneous nodes be adhered and it guarantees high scalability and security against attacks (Basagni *et al.*, 2004)2004.

Several studies have shown the possibility of DoS and DDoS attacks and the high bandwidth consumption, attributed to Gnutella query flood mechanism (Exploiting the security weaknesses of the gnutella protocol. http://www.cs.ucr.edu/ csyiazti/courses/cs260-2/project/gnutella.pdf.), (Marina & Das, 2001), (Das, et al., 2000). While it has generally assumed that the risk of downloading malware in Gnutella is not higher than any other P2P network (Hoven *et al.*, 2005)2005, the analysis of several other P2P systems shows that none appear to be similarly populated with noxious content. The fake query results camouflage malicious content as a specific filename and/or attribute matching the query request. This induces the requesting peer to download the file. The incorrect results methodically routed back in response to each query request suggests a constant presence inside the system of malicious peers, who must have some incentives in cheating and spreading big quantities of unsolicited content (Exploiting the security weaknesses of the gnutella protocol. http://www.cs.ucr.edu/ csyiazti/courses/cs260-2/project/gnutella.pdf.). Many papers address Gnutella security through building reputation systems (Cornelli *et al.*, 2002), (Hatsuda & Motozumi, 1998)IEEE Transactions on</secondary-title></titles><periodical><full-title>Aerospace and Electronic Systems, IEEE Transactions on</full-title></periodical><pages>23-32</pages><volume>34</volume><number>1</number><dates><year>1998</year></dates><isbn>0018-9251</isbn><urls></urls></record></Cite></EndNote>, integrating market-based models of misaligned incentives, (Alaettinoglu *et al.*, 1991)1991,(Srour *et al.*, 2006) or departing from a purely decentralized architecture (Lui *et al.*, 2002).

Security is even a big issue in latest Gnutella protocol version, as no countermeasures have been adopted to overcome some of the security concerns highlighted above. The only security measures and tools currently available in some servents are: First, A manual block-host feature, which blacklists specific IP addresses. Second, manual content filtering, which prevents query results with specific keywords from being displayed.

Both tools are clearly interim, not robust solutions, as they are manual and single-host based. They are ineffective and do not offer any real protection. Additionally, even if an IP address is blacklisted by a node, the query result coming from that host address is still routed, since the other nodes have no knowledge of which IP addresses or keywords the requester wishes to block, thus the waste of resources, as traffic generated by malicious query replies, remains same. Content filtering is equally ineffective, as it is based on filenames in query results, which are dynamically modified and camouflaged by malicious peers. This effectively bypasses keyword filtering.

1.2 Intrusion Detection Systems (IDS)

Amongst worm defensive mechanisms, IDSs (Abdelhaq *et al.*, 2012)2012 {Abdelhaq, 2012 #503}{Abdelhaq, 2012 #503}are the most widely deployed techniques that utilize the self-duplicating repetitive nature of computer worms to detect the patterns and signatures of theses malicious codes in the network traffic. Some of the IDS functionalities are: Monitoring and analyzing both user and system activity, Analyzing system configurations and vulnerabilities, Assessing system and file integrity, Ability to recognize typical attacks patterns, Analysis of abnormal activity patterns, and Tracking user policy violations. These systems based on the parameters used for detection, can be broadly divided to Signature-based IDS (SIDS) and Anomaly-based IDS (AIDS) systems (Uddin *et al.*, 2010).

1.2.1 Signature-based IDS (SIDS)

Signature-based detection is normally used for detecting known attacks (Kruegel & Toth, 2003). No knowledge of normal traffic is required but a signature database is needed for these types of detection systems. For worm detection, this system does not care how a worm finds the target, how it propagates itself or what transmission scheme it uses. The system takes a look at the payload and identify whether or not it contain a worm. One big challenge of SIDS is that every signature requires an entry in the database, and so a complete database might contain hundreds or even thousands of entries. Each packet is to be compared with all the entries in the database. This can be very resource consuming and doing so will slow down the throughput and making the IDS vulnerable to DoS attacks. Some of the IDS evasion tools use

this vulnerability and flood the SIDSs with too many packets to the point that the IDS cannot keep up with the traffic, thus making the IDS time out and drop packets and as a result, possibly miss attacks (Alder *et al.*, 2004). Further, this type of IDS is still vulnerable against unknown attacks as it relies on the signatures currently in the database to detect attacks.

1.2.2 Anomaly-based IDS (AIDS)

AIDSs detect abnormal behaviors and generate alarms based on the abnormal patterns in network traffic or application behaviors. Typical anomalous behaviors that may be captured include: First, misuse of network protocols, such as overlapped IP fragments and running a standard protocol on a stealthy port. Second, Uncharacteristic traffic patterns, such as more UDP packets compared to TCP ones. Finally, Suspicious patterns in application payload. The biggest challenges faced by AIDS is defining what a normal network behavior is, deciding the threshold to trigger the alarm, and preventing false alarms. The users of the network are normally human, and people are hard to predict. If the normal model is not defined carefully, there will be lots of false alarms and the detection system will suffer from degraded performance.

1.3 The Human Immune System (HIS)

The Human Immune System (HIS) is a network of cells, tissues, and organs that work together to defend the body against attacks by "foreign" invaders (Parham & Janeway, 2005). The immune system is amazingly complex. It can recognize and remember millions of different enemies, and it can produce secretions and cells to match up with and wipe out each one of them. There are two major branches of immune system, Innate and Adaptive. The former Innate Human Immune Systems (IHIS) is an unchanging mechanism that detects and destroys certain invading organisms (Creely *et al.*, 2007)2007. These systems form the first line of defense against microbes and consist of cellular and biochemical defensive mechanisms that exist even before infection and are ready to response to infections quickly. The latter Adaptive Human Immune Systems (AHIS) is responds to previously unknown foreign cells and builds a response to them that can remain in the body over a long period of time (Parham & Janeway, 2005). This remarkable information processing biological system has caught the attention of computer science in recent years (Aickelin & Dasgupta, 2004). These systems evolve in response and also proportionate to infections. Apparent features of adaptable immunity systems are: Enormous response to definite molecules, The ability to remember and stronger response to continual collision to a special kind of microbe (Elson *et al.*, 2002)2002,(Li Xiao, et al., 2005). In addition, an Artificial Immune Systems (AIS) is introduced to be an adaptive system, inspired by theoretical immunology and observed immune functions, principles and models, which are applied to problem solving. They are systems developed using the HIS as inspiration, rather than creating a comprehensive model, in an attempt to capture some or all of the features it provides. In most instances however, only a few principles from immunology are used. Table 1 shows the mapping of HIS with Gnutella P2P network.

Table 1. *Mapping of HIS with Gnutella P2P network*

Human immune system	Gnutella P2P network
Bone marrow & thymus	IDS
Primary lymphoid organs	Leafpeer
Secondary lymphoid organs	Ultrapeer
Antibody	Detector
Antigen	Intrusion
Self	Normal traffic
Nonself	Abnormal traffic

1.4 Mapping of DDoS attacks with HIS

The features of distributed systems and different mechanisms of HIS are directly proportional to each other and disclose similarities between these two seemingly different contexts. The similarities are inspired by HIS to identify effective intrusion in distributed systems (Aickelin *et al.*, 2004), (Bentley & Kim, 2001), (de Paula *et al.*, 2004). DDoS attacks are large and increasing threat to the Internet community. The need to protect against and mitigate the effects of DDoS attack has been recognized by both the commercial and research community for some years. A DDoS attack response must be quick; much quicker than picking up the phone and calling system administrators autonomous system. DD-police protects Gnutella P2P network against DoS model. Due to the dynamic nature of P2P network, nodes leave and join the network arbitrary that increase system's overload (Athanasopoulos *et al.*, 2006).

While in the context of exploiting the features of HIS mapped to DDoS attacks in the security of computer networks, Forrest performed the first research to discriminate between self and nonself in network AIS. Hofmeyr designed an AIS, called ARTIS (Hofmeyr & Forrest, 2000). This system is not very efficient because collaboration and information exchange among nodes is not considered and intrusion detection is done separately in each computer. LISYS is one of the first structures for AISs that is designed for a simple local network and can learn network traffic and identified anomaly traffic (Hofmeyr & Forrest, 2000). On the other hand, Cfengine system proposed to automatically configure large number of systems on heterogeneous nodes (Greensmith & Aickelin, 2008). Furthermore, as long as a new discordance does not happen, the IDS is passive. In order to increase scalability, Cfengine IDS updates the average system efficiency, the number of each service input and output connection and packet characteristic (Aickelin *et al.*, 2003),(Greensmith & Aickelin, 2008), (Cayzer & Aickelin, 2002). Results of Cfengine show that danger signal potentially affects false positive rate and also memory detectors improve detection rate.

The stratagem to resolve security vulnerabilities problems in P2P network is to use IDSs. By employing IDS at different layers in the network, it is possible to detect suspicious ways and potential attacks in Gnutella hybrid P2P networks. These security breaches can be trounce by firstly preventing the network form intrusions and if it does not works then, the second defensive line is to apply and implement IDSs in the network to detect intrusions. As distributed networks continuously change their structure by applying different topologies inside the network, the strategies to detect intrusions are also changing gradually, it is therefore becomes essential that IDS system be dynamic in nature to meet the ever changing demands of the security constraints with passage of time (Uddin, et al., 2010).

1.5 Apparent Features of AHIS Responses

The typical problems amenable to being solved by AISs are security vulnerability issues in P2P networks suing IDS systems and Data Mining issues using collaborative filtering and clustering (Aickelin & Dasgupta, 2004). All humoral and cellular immunity systems responses against foreign antigens that have some basic features that characterize the lymphocytes that creates this response (Elson, et al., 2002), (A. Okine *et al.*, 1997), (Melby, 2005). Generally, the features of HIS that are applied in the proposed system to solve real world problems are: Variety and adaption, Immunological memory and protection against auto-immune attacks such as contractions and homeostasis as well as Major histocompatibility cells (Dasgupta *et al.*, 2003).

In the former Variety and adaption feature, the total number of lymphocytes antigenic features in a person called lymphocyte repertoire are in great number. This feature of lymphocyte repertoire is called variety that is the outcome of diversity in the structures of connection areas to the antigen in lymphocyte antigenic receptors in terms of the antigenic receptors structure and consequently antigenic features. In the proposed system, when an attack template is detected, it is forwarded to all connected ultrapeers in the network. Then, the proposed genetic algorithm will be applied for optimizing the attack template. The proposed algorithm then will be applied to all detected templates and are collectively known as attack dataset and the whole process is called variety. On the other hand, in the immunological memory feature, the collision of an immunity system to a foreign antigen increases its ability to respond to the same antigen again. The responses that are created against the second or next collisions to a kind of antigen are called secondary immunity responses and usually are faster and stronger than the first immunity response against the same kind of antigen. These memory cells have specific features that cause them to operate more effectively, in response to an omission of antigen, than naive lymphocytes that had previous collision to them.

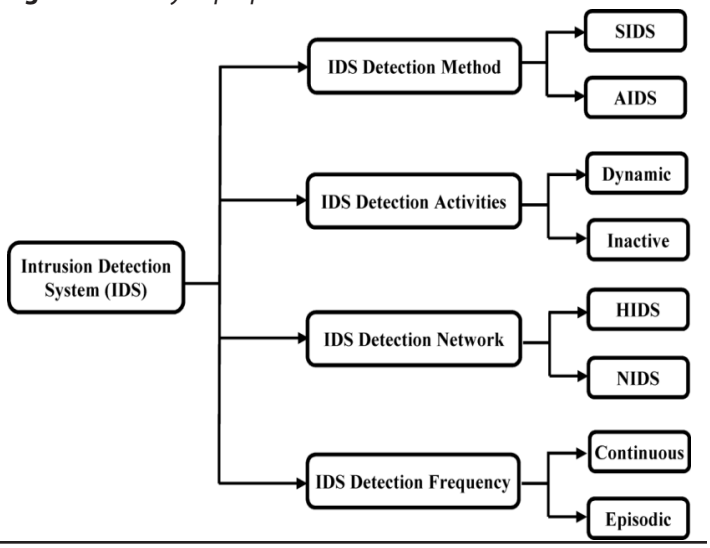
In the contractions and homeostasis feature, after the simulation of antigen, all natural immune responses decrease as the time progresses. Therefore, the immune system returns to repose state and this trend is called constancy or homeostasis. The omission of stimulus causes the death of lymphocytes by means of apoptosis. If the same mechanism is applied in P2P networks, then after detecting the attack, leaf peers go to the suspended mode until the network becomes stable called repose state. Furthermore, in the latter Major Histocompatibility Cells (MHC), major activities of T-lymphocytes consists defense against in-cell microbes and activation of other cells such as macrophage and B-lymphocytes. Therefore, the recognition of transplant as self or nonself is a genetic feature. Those genes that are in charge of receiving the transplanted tissues as self or nonself are called histocompatibility between people. All MHC molecules have some specific and common features that are of great importance in presentation of antigen and its recognition by T-lymphocytes. In the proposed system, negative selection algorithm for training phase running on all leafpeers also uses the same MHC properties of the HIS.2.

2. Materials and Methods

2.1 Proposed IDSs based on Genetic Algorithm

The proposed IDS use AIS to define different algorithms. The proposed system defines its operations in several levels with heterogeneous function of peers. The proposed IDS consist of combination of different algorithms used to investigate security breaches in Gnutella hybrid P2P networks. It uses both SIDS and AIDS techniques with combination of AIS to detect different attacks templates. The proposed IDS will be located in all leafpeers in Gnutella hybrid P2P network; the system detects and announces the existence of attack or presence of intrusions to other ultrapeers ultrapeers by means of distributive ultrapeer warning. Consequently, the stated system discovers the network intrusions by cooperation between leafpeer and Ultrapeer. To explain the working of the proposed system, it will be explored from four different aspects. These aspects are: IDS Detection Method, IDS Detection Activities, IDS Detection Network, and IDS Detection frequency. Figure 1 presents the taxonomy of the proposed IDS.

Fig.1. *Taxonomy of proposed IDS*



2.1.1 IDS Detection Method

IDS distinguish between SIDS and AIDS detections. To detect the intrusion, algorithms of AIS like negative selection and clonal selection will be used to achieve the desired objectives (J. Kim & P.J. Bentley, 2001). In fact, new and unknown attacks are detected. Anomaly traffic and normal traffic are distinguished using danger theory (Aickelin, et al., 2003; Cayzer & Aickelin, 2002). The proposed system is designed by combining the negative and clonal selection techniques. In the training phase, AIDSs will be used to detect abnormal behaviors while in the testing phase SIDS will be used to actually detect the intrusions.

2.1.2 IDS Detection Activities

With the saturation of network resources in a short time and prediction of attack possibility, the node (leafpeer or ultrapeer) in the suggested IDS system warns its ultrapeers to confront attacks. Therefore, on surrounding ultrapeer become aware of possible attacks. Invaded peers would be suspended since they are not resistant against attack and they are protected to some extent. This system has an active attitude by detecting and announcing leafpeer and ultrapeer new behaviors.

2.1.3 IDS Detection Network

IDS can be divided into multiple groups depending on the type of network to be used for performing the detection. In Gnutella hybrid P2P networks, IDS are categorized into two main categories i.e. Network-based Intrusion Detection System (NIDS and Host-based Intrusion Detection System (HIDS). NIDS is installed on the network's gateway and examines the traffic of the network from which it passes. Since ultrapeer in Gnutella hybrid P2P network plays the role of gateway and distinguishes anomaly traffic from normal traffic. The ultrapeer sends attack strategy to other ultrapeers after identifying and proving attack.

HIDS performs on different nodes based on collecting network traffic information. These pieces of information are separately analyzed in each node and the results are used to immune the activities of the aforementioned node. Obviously, the proposed IDS is located on all leafpeers, so it performs distributive. The results generated, informs other nodes of the existence of attacker nodes.

2.1.4 IDS Detection Frequency

Leafpeers perform intrusion detection continuously while ultrapeers would be active only when sending the "Stress message" from leafpeers. The proposed system uses different functions to detect intrusion especially DDoS attack which is the main focus of this paper. Each peer does more than one function, like creating alarm in the proposed system, a process should be followed that requires several functions clarified in section 2.2.

2.2 Development of new Generation of Detector (Genetic Algorithm)

The templates with most conformity of attacks are most likely to happen again in near future and such templates are used in the selection phase of genetic algorithm. In fact ranking method is used, in a way that detectors are ranked based on number of conformity and then template selection would be done according to the rank based fitness. It is important to use a competitive method to select best attack templates for selection. This method works in a way that a small subcategory of attack templates is randomly chosen and then competes together. Finally in this competition, one of them is chosen based on affinity level (Jian *et al.*, 2004). After selecting best templates (with more conformity) by crossover operator and with the purpose of producing better templates, new templates would be created. After the function of attack templates crossover, mutation includes the change of zero to one. On the other hand, the function is applied in a lymphocyte repertoire to protect the different forms of the distinctness of attack templates.

2.2.1 Artificial Immune Algorithm

As HIS performs actively and distributively, AIS algorithms are particularly used in proposed IDS system to develop the purpose specified. The major features of HIS are inspected to detect intrusion and how it reacts against intrusions (Chang, 2002),(Melby, 2005). It will be used in Gnutella hybrid P2P network to confront DDoS attacks. In the proposed IDS system negative selection algorithm is used in training phase and it function as follows:

2.2.2 Negative Selection Algorithm

Gnutella network packets are captured by *tcpdump* monitoring tool (Mills *et al.*, 2010)2010 and *gtk-gnutella* file sharing software (Kim *et al.*, 2009)2009. These packets are considered as self-dataset. After that some detectors (immature detectors) are produced by random Gaussian function and by comparing these two datasets, any detector that do not correspond to the normal network traffic will be added to the detectors' list as nonself detector (mature detectors). In this stage, the number of detectors is investigated. If this number increases, the accuracy of detection goes up and computational overload increases too (J. Kim & P.J Bentley, 2001),(Cannady & Gonzalez, 2004).

After receiving each Gnutella packet, the source IP address, the local destinations IP address and average time interval between two consecutive sent packets will be added to the template. Then the size of bandwidth occupied will be examined. If it does not reach the default threshold, the template will be faded out of existence and a new template will be made. Otherwise, the possibility of attack occurrence will be announced to connect ultrapeers. Leafpeer after making sure of the existence of each ultrapeer sends the template of possible attack to each ultrapeer. In this stage, leafpeer announces the possibility of attack occurrence

and distinguishes between abnormal traffic and normal traffic. Leafpeer will be suspended for a definite time span to prevent the reception of any packet or message. When this time span ends, leafpeer will return to its initial state.

Ultrapeer announces its existence to leafpeer by receiving the possibility of attack occurrence and after receiving the template of possible attack, will compare with nonself dataset. If the template conforms to each detector, ultrapeer broadcasts it to other ultrapeers as a detector. Then ultrapeer creates conformed detectors once again, increases their affinity and if detectors aren't conformed, ultrapeer will change its main structure according to the number of conformities, detector state changes from mature stage type and beneficial life time is inspected. As each kind of detector has a definite lifetime, those detectors whose lifetime is ended are deleted from detectors dataset. The negative selection algorithm is stated below in Table 2.

Table 2. *Negative Selection Algorithm*

Use gtk-gnutella file sharing to produce Gnutella normal traffic
Use tcpdump monitoring tools to capture packets
G_{nd} ← Gnutella normal dataset
G_{ad} ← Gnutella abnormal dataset detector dataset)
d ← detector
D_{th} ← Threshold of detector
1: while number of d less than D_{th}
2: d← create immature detector with uniform Gaussian random function
3: if G_{nd} contains d then
4: drop d
5: else
6: d insert into G_{ad}
7: end if
8: end while

The genetic algorithm is used to improve detectors in the proposed system. Genetic algorithm also causes variety in nonself templates in active stage, in a way based on clonal selection algorithm, those cells that identify detector grow and those cells that are not able to identify detector die. As leafpeer and ultrapeer operate in a collaborative and parallel manner and available network peers are fully distributed, leafpeer and ultrapeer's function are separately inspected as given in Table 3 and Table 4.

Table 3. *Leafpeer Function (Test Phase)*

G_p: Gnutella Packet
BW_d: percentage of leafpeer Bandwidth depletion
BW_{th}: Threshold of leafpeer Bandwidth depletion
01: While peer is in active mode
02: T← receive features of new G_p
03: if $BW_d \geq BW_{th}$ then
04: forwards msg-stress along connected ultrapeers
05: else
06: Drop T
07: end if
08: if received msg-stress reply then
09: forwards T to certain ultrapeers
10: stand in suspend mode for time span
11: end if

Table 4. *Ultrapeer Function (Test Phase)*

T_a: Template of attack
T_c: number of conformity with T_a
T_{ttl}: time to live for every detector
01: while ultrapeer is in active mode
02: T← receive G_p
03: if G_p.Type is msg_stress then
04: forwards msg_stress reply along leafpeer
05: end if
06: T_a← received msg_template
07: if G_{ad} contains T_a then
08: increment T_c
09: set T_{ttl} to zero
10: update G_{ad} with T_a
11: forward T_a along every ultrapeers in network
12: Run GA .Algorithm on G_{ad}
13: end if

2.3 Experimental Methodology

This section presents different aspects of the experimental methodology of the proposed system process, such as creation of template, sending and receiving of attack template, identification of attack based on received template, sending attack template to other ultrapeers, attack type classification, and threshold value limit. Furthermore, the analysis of the DDoS attack and simulation preliminaries are also presented and highlighted.

2.3.1 Creation of Template

Leafpeer records the templates of messages it receives in a short time span but if the volume of received messages is more than the threshold value specified in that particular time span then, a new template will be formed containing information related to source IP address, the destination IP address (local) and

the time interval between Gnutella packets and will be sent as the template of possible attack; otherwise the produced template be out aside.

2.3.2 Sending & Receiving of Attack Template

After an attack, leafpeer forms a template; other peers in the network are informed about the possible occurrence of this attack. If ultrapeer returns Stress Reply message, leafpeer will inform about possible attack occurrence by sending Stress message to all peers. The possible attack template is sent to ultrapeer by template message.

2.3.3 Identification of Attack based on Received Template

After receiving the possible attack template using Template message, ultrapeer starts the activity of conforming received template to the template of available attacks in dataset. 30 percent conformity shows that an attack has happened.

2.3.4 Sending Attack Template to other Ultrapeers

When an attack is diagnosed and confirmed, the ultrapeer sends the attack template to other ultrapeers, so that they would be informed of the occurrence of the attack and they should increase their detection rate.

2.3.5 Classification of Attack Type

After an attack has been confirmed the next step is to classify it between anomaly traffic and normal traffic. An attitude should be chosen that by receiving numerous Gnutella messages in definite time intervals and saturating bandwidth, considers the peer sent traffic as attack traffic or anomaly traffic. The classification of an attack is a two steps process, in first step leafpeers distinguish between normal traffic and possible abnormal traffic. This process is called discrimination self/nonself (Forrest *et al.*, 1994). While in the second step, ultrapeers distinguish between possible normal traffic and abnormal traffic; this process is done by applying danger theory (Cayzer & Aickelin, 2002),(Gnutella website. http://www.gnutella.com).

2.3.6 Threshold Value Limit

If the number of message sent are more than bandwidth occupied, threshold value and attack occurrence is announced as well then, sending and receiving message to the ultrapeer can be prevented and the rate of sent messages can be reduced by adopting some measures. In fact invaded peers would be suspended since they are not resistant against attack and they are protected to some extent, in a way that they just accept high priority packets that are sent by surrounding ultrapeers.

2.3.7 DDoS Attack Analysis

DDoS attacks are a flooding attack of many attacking hosts (agents) with distributed and coordinated control, along with one or more attackers controls the handlers while each handler controls multiple agents. Handlers and agents are extra layers introduced to increase the rate of packet traffic as well as to hide the attackers from view. Each agent can choose the size and type of packets as well as the duration of flooding. While the victim may be able to identify some agents and have them taken offline, the attacker can monitor the effects of the attack and create new agents accordingly (Dietrich *et al.*, 2000). To simulate the results, a discrete event simulator will be used to simulate the results of Gnutella P2P file sharing. Gnutellasim is suitable for Gnutella network and is installed on PDNS and ns 2.27. In order to evaluate the suggested system, *gtk-gnutella-0.96.8-2* file sharing client (Kim, et al., 2009) and *tcpdump-4.1.1* monitoring software (Mills, et al., 2010) is used to generate and record Gnutella traffic.

2.3.8 Simulation Preliminaries

One challenge in intrusion detection is finding moral data sets for experiments and testing. Our objective is to control the dataset; we chose to collect data from an internal restricted Gnutella P2P network. In this environment, we can understand all of the connections, and limit the DDoS attacks. We install firewall of ISA server in the entrance of our network. Then external connections must pass through a firewall. The dataset used for performing the experiments and analysis is related to Gnutella P2P network traffic. The proposed scenario includes 23 peers that are divided into 5 ultrapeers and 18 leafpeers.

3. Results and Discussion

Gnutella Protocol v. 0.6 will be used for performing the simulations. In IDS, self is defined, as the set of normal pair wise TCP/IP connections between leafpeer and ultrapeer and nonself is the set of connections. When enormous numbers of Gnutella packets are transmitted over the network they are not observed normally on the network. The efficiency of proposed system is analyzed based on the following criteria:

3.1 Negative Selection Time

Some immature detectors are produced by random Gaussian function and this dataset compares with Gnutella normal dataset. If any detectors do not match with normal traffic template, it will be added to the mature detectors' list. Output of training file is a mature detectors' dataset. Figure 2 shows the time of negative selection in proportion to the number of detectors. By increasing the number of mature detectors, negative selection time will be increase too but detection precision is optimized. Because of using genetic algorithm, the time of negative selection is more beneficial than LISYS algorithm.

3.2 Detection Precision

In order to increase the detection precision, false positives should be reduced. This research will identify parameters that appear most important for minimizing false positives, as well as how to maximize the percentage of detecting intrusions. The percentage of attack detection will be measured by proportion of discovered attack occurrences to all attack occurrences as shown in equation 1.

$$R_{dt} = \frac{T_d}{T_a} \times 100 \quad (1)$$

where R_{dt} denotes the corresponding false positives rate. T_d is the number of attacks that be discovered and T_a is the total number of attacks.

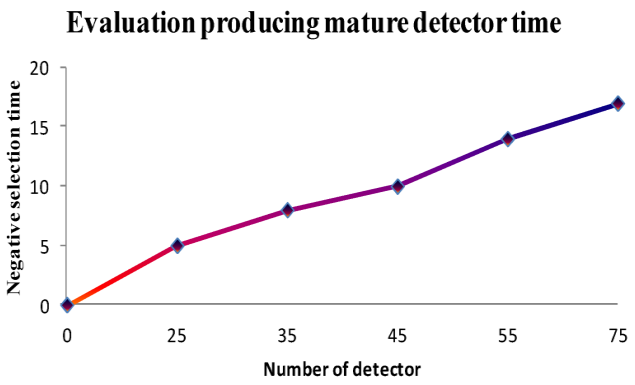
In fact, false positive is the sending of alarm message by IDS in the time that attack has not happened and its calculated as shown in equation 2.

$$R_{fp} = \frac{T_p}{T_a} \times 100 \quad (2)$$

where T_d is the total number false positive alarms and T_a is the total number of attacks.

The proposed system is adopted to describe the tradeoff between the detection rate and false positive rate. Therefore, we evaluate the best attitude coherent to these factors for yielding optimum resolves.

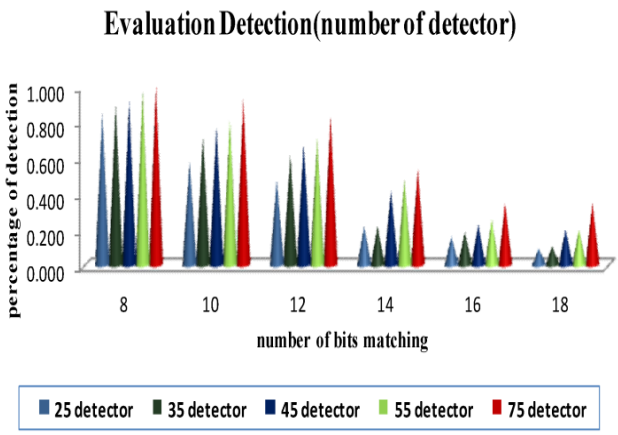
Fig.2. *Production Time of Mature Detector*



3.3 Number of Detectors

To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.4 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in number of different conformity bits. With increase in number of detectors, the percentage of attack discovery goes up on the one side and the false positive increases on the other side. In a way that in all the forms of conformity bits, 75 detectors show the most efficient response for detecting attack. But due to computation over load, the number detectors are commonly not very high. In LISYS algorithm, the number of detectors is 100. Figure 3 illustrates the evaluation detection with respect to the number of detectors.

Fig.3. *Detection with different number of detectors*



3.4 Bit Matching Algorithm

Some detectors in this IDS system are usually implemented as strings, whose function is to classify new strings as normal or abnormal by matching them in some forms. The perfect matching is rare in the immune system. So, we use a partial matching rule known as r-contiguous bits matching. Under this rule, two strings match only if they are identical in at least 'r' contiguous locations.

Our observations in Figures 4 and 5 show that immune system as inspiration for detecting intrusion is the best approach. To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.6 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in the number of different conformity bits. The number of strings a detector matches increases exponentially as the value of r decreases. For example, 8 conformity bits is the best resolve for attack detection rate but is the worst result for false positive rate. After checking these factors, we use 12 conformity bits and LISYS algorithm to elect the number.

Fig.4. *Evaluation Detection*

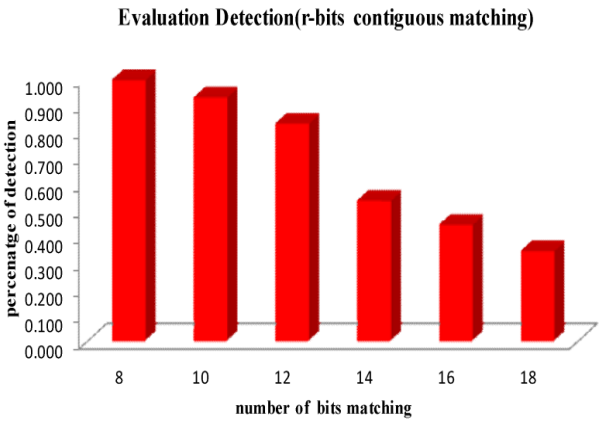
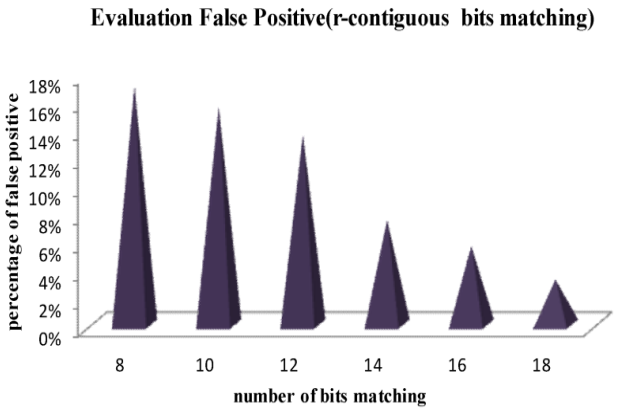


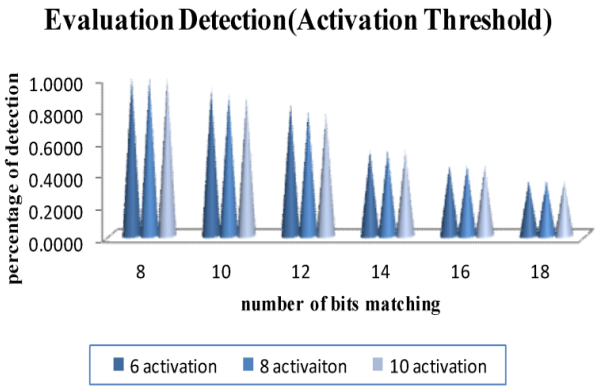
Fig.5. *Evaluation of False Positives*



3.5 Activation Threshold Values

Activation threshold shows detector's condition in mature, active and memory state. Activation thresholds are a mechanism designed to reduce false positives. To test our expectations, we studied the effect of changing the activation threshold on the number of false positives. These experiments were run with different 'r' values. The proper amount of activation threshold is evaluated with 75 detectors, crossover operator 0.6 and mutation operator 0.005. In fact the less this amount, the sooner the detector goes to the activation stage, therefore generation production will be more and the better discovery will occur. Also this parameter decreases the false positive. 6 and 8 activation threshold has the same attack discovery percentage with small differences. For the number of conformity bits 16, 14 and 18, the activation threshold of 8 is better but LISYS algorithm suggests 10 activation thresholds. Figures 6 and 7 illustrates how the number of false positives lessens as the activation threshold increases.

Fig.6. *Evaluation Detection*



As Gnutella P2P network has two versions: Gnutella 0.4 and Gnutella 0.6. In Gnutella 0.6 networks, peers with high processing strength are used called ultrapeers. So in this system, both versions of Gnutella P2P network with one-point crossover operator and two-point crossover operator are examined for intrusion detection (M. Foster & Ripeanu, 2002), (Beverly Yang & Garcia-Molina, 2003), (Stepney *et al.*, 1974), (Lee & Stolfo., 2000). Simulation results indicate the superiority of intrusion detection in Gnutella 0.6 hybrid P2P network by two-point crossover operator in comparison to other forms. As the number of detectors increases, more attacks will be discovered. Figures 8 and 9 denote comparison of two versions Gnutella network by different crossover operator.

Fig.7. *Evaluation of False Positives*

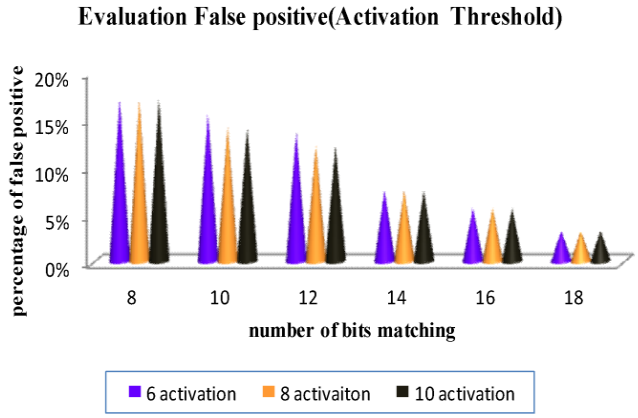


Fig.8. *Comparison of attack detection percentage to number of detectors for Gnutella 0.4*

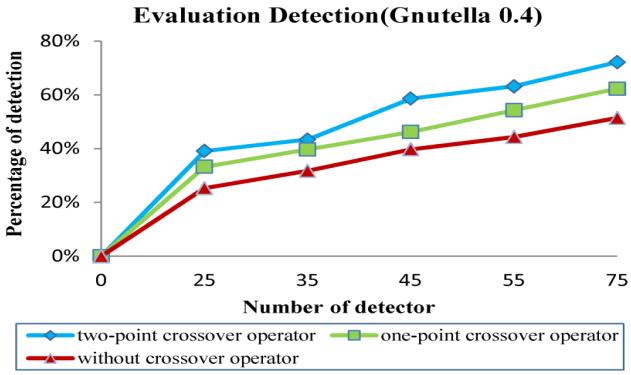
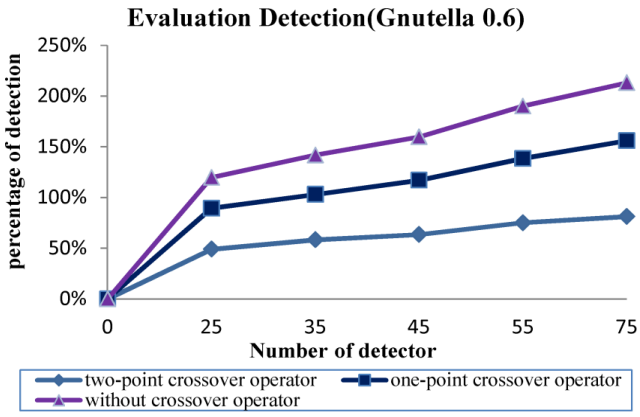


Fig.9. *Comparison of attack detection percentage to the number of detectors for Gnutella 0.6*



3.6 Delay

The time of attack occurrence in proportion to the time that IDS reacts against attack. In the proposed IDS system, the average identification time of each attack is 15 seconds.

4. Conclusion

The proposed IDS based on HIS uses SIDS and AIDS techniques. Each time an attack is identified, a new set of generation is added to the detectors dataset. As false positives decrease, attach detection increases. Thus the overall detection rate increases which ultimately increases the functional efficiency of the network to an acceptable level. In addition, the proposed IDS system inspects nodes cooperation and provides an efficient way of properly using the algorithms of AIS. The simulation results clearly show that the proposed method not only has adaptability, scalability, flexibility and variety but also has high accuracy and correctness.

5. Acknowledgement

This research was supported in part by the Centre for Research and Instrumentation Management (CRIM), University Kebangsaan Malaysia, Malaysia. Grant: UKM-GUP-2012-089.

6. References

1. A. Okine, Dasgupta D and Nii. (1997). Immunity-based systems: A survey. Paper presented at the Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics.
2. Abdelhaq M, Hassan R and Ismail M. (2012). A Study on the Vulnerability of AODV Routing Protocol to Resource Consumption Attack. Indian Journal of Science and Technology, 5(11), 3573-3577.
3. Aickelin U, Bentley P, Cayzer S, Kim J and McLeod J. (2003). Danger Theory: The Link between Artificial Immune Systems and Intrusion Detection Systems. Paper presented at the Proceedings of the 2nd International Conference on Artificial Immune Systems.
4. Aickelin U and Dasgupta D. (2004). An Immune-Inspired Approach to Anomaly Detection: University of Nottingham, Nottingham.
5. Aickelin U, Greensmith J and Twycross J. (2004). Immune system approaches to intrusion detection–a review. Paper presented at the Proceeding of the Third International Conference on Artificial Immune Systems. Number 3239 in Lecture Notes in Computer Science.
6. Alaettinoglu C, Shanker AU, Dussa-Zieger K and Matta I. (1991). Mars (maryland routing simulator)-version 1.0 user's manual. University of Maryland College Park Technical Report, 91(80), 1-36.
7. Alder JBR, Doxtater A, Foster J, Kohlenberg T and Rash M. (2004). Snort 2.1Intrusion Detection (2nd ed. ed.): Rockland, MA: Syngress (Distributed by O'Reilly and Associates).
8. Andrade N, Brasileiro F, Cirne W and Mowbray M. (2007). Automatic grid assembly by promoting collaboration in peer-to-peer next term grids. International Journal of Critical Infrastructures, 67(8), 957-966.
9. Athanasopoulos E, Anagnostakis K and Markatos E. (2006). Misusing unstructured p2p systems to perform dos attacks: The network that never forgets. Paper presented at the Proceedings of the 4th International Conference on Applied Cryptography and Network Security (ACNS'06).
10. Basagni S, Conti M, Giordano S and Stojmenović I. (2004). Mobile ad hoc networking: Wiley-IEEE Press.
11. Bentley PJ and Kim J. (2001). Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection. Paper presented at the The Congress on Evolutionary Computation (CEC-2001), Seoul, Korea.
12. Berners-Lee T, Hendler J and Lassila O. (2001). The semantic web: A new form of web content that is meaningful to computers will unleash a revolution of new possibilities Scientific American.
13. Beverly Yang B and Garcia-Molina H. (2003). Designing a super-peer network. Paper presented at the Proceeding of 19th International Conference on Data Engineering,.
14. Broch J, Maltz DA, Johnson DB, Hu YC and Jetcheva J. (1998). A performance comparison of multi-hop wireless ad hoc network routing protocols. Paper presented at the Proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM'98).
15. Cannady LJ and Gonzalez J. (2004). A self-adaptive negative selection approach for anomaly detection. Paper presented at the Proceedings of the 2004 Congress of Evolutionary Computation.
16. Cayzer S and Aickelin U. (2002). Danger theory and its applications to AIS. Paper presented at the Proceeding of the Second Internation Conference on Artificial Immune Systems (ICARIS-02).
17. Chang RKC. (2002). Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A tutorial. IEEE Communications Magazine, 40(10), 42-51.
18. Cornelli F, Damiani E, Capitani SD, Paraboschi S and Samarati P. (2002). Implementing a Reputation-Aware Gnutella Servent. Lecture Notes In Computer Science, Springer-Verlag, London, UK, 2376, 321-334.
19. Creely SJ, McTernan PG, Kusminski CM, Da Silva N, Khanolkar M, Evans M, Harte A and Kumar S. (2007). Lipopolysaccharide activates an innate immune system response in human adipose tissue in obesity and type 2 diabetes. American Journal of Physiology-Endocrinology And Metabolism, 292(3), E740-E747.

20. Das SR, Castañeda R and Yan J. (2000). Simulation-based performance evaluation of routing protocols for mobile ad hoc networks. Mobile networks and applications, 5(3), 179-189.

21. Dasgupta D, Ji Z and Gonzalez F. (2003). Artificial immune system (AIS) research in the last five years. Paper presented at the The 2003 Congress on Evolutionary Computation, 2003. CEC'03. .

22. de Paula FS, de Castro LN and de Geus PL. (2004). An intrusion detection system using ideas from the immune system. Paper presented at the roceeding of IEEE Congress on Evolutionary Computation (CEC-2004).

23. Dietrich S, Long N and Dittrich D. (2000). Analyzing distributed denial of service tools: The shaft case. Paper presented at the Proceedings of USENIX (Dec 2000).

24. Dubendorfer T and Wagner A. (2003). Past and Future Internet Disasters: DDoS attacks: April.

25. Elson J, Girod L and Estrin D. (2002). Fine-grained network time synchronization using reference broadcasts. ACM SIGOPS Operating Systems Review, 36(SI), 147-163.

26. . Exploiting the security weaknesses of the gnutella protocol. http://www.cs.ucr.edu/ csyiazti/courses/cs260-2/project/ gnutella.pdf.

27. Forrest S, Perelson AS, Allen L and Cherukuri R. (1994). Self-Nonself Discrimination in a Computer. Paper presented at the Proceeding IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press.

28. Foster I, Kesselman C and Tuecke S. (2001). The anatomy of the grid: Enabling scalable virtual organizations. The International Journal of High Performance Computing Applications, 15(3), 200-222.

29. Foster M and Ripeanu I. (2002). Mapping the Gnutella network. Paper presented at the Proceeding of the 1st International Workshop On Peer-to-Peer Systems, Cambridge, MA.

30. G.Oikonomou, Reiher P, Robinson M and Mirkovic J. (2006). A framework for a collaborative DDoS defense. Paper presented at the Proceedings of the 2006 annual computer security applications conference.

31. . Gnutella website. http://www.gnutella.com

32. Gomes. (2001). Gnutella keeps growing and growing Online. WSJ Interactive Edition, http://www.zdnet.com/zdnn/ stories/news/0,4586,2766234,00.html. May2001. .

33. Greensmith J and Aickelin U. (2008). The deterministic dendritic cell algorithm. Paper presented at the Proceeding of the 7th International Conference on Artificial Immune Systems (ICARIS).

34. Greensmith J, Twycross J and Aickelin U. (2006). Dendritic cells for anomaly detection. Paper presented at the Proceeding of the Congress on Evolutionary Computation (CEC).

35. Hatsuda T and Motozumi Y. (1998). Interference experiments between fixed-satellite and terrestrial radio-relay services. Aerospace and Electronic Systems, IEEE Transactions on, 34(1), 23-32.

36. Hofmeyr SA and Forrest S. (2000). Architecture for an artificial immune system. Evolutionary computation, 8(4), 443-473.

37. Hoven N, Tandra R and Sahai A. (2005). Some fundamental limits on cognitive radio. Wireless Foundations EECS, Univ. of California, Berkeley.

38. Hwang K, Cai M, Kwok Y-k, Song S, Chen Y and Chen Y. (2006). DHT-based security infrastructure for trusted internet and grid computing. International Journal of Critical Infrastructures, 2(4), 412-433.

39. Jian G, Da-Xin L and Bin-Ge C. (2004). An induction learning approach for building intrusion detection models using genetic algorithms. Paper presented at the Proceedings of Fifth World Congress on Intelligent Control and Automation WCICA.

40. Johnson DB, Maltz DA and Broch J. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc networking, 5, 139-172.

41. Katz ML and Shapiro C. (1994). Systems Competition and Network Effects. Journal of Economic Perspectives, 8(2), 93-115.

42. Kim J and Bentley PJ. (2001). Evaluating negative selection in an artificial immune system for network intrusion detection. Paper presented at the Proceedings of GECCO

43. Kim J and Bentley PJ. (2001). Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator. Paper presented at the Proceedings of the 2001 Congress on Evolutionary Computation.

44. Kim RY, Kwak JS and Etemad K. (2009). WiMAX femtocell: requirements, challenges, and solutions. Communications Magazine, IEEE, 47(9), 84-91.

45. Kruegel C and Toth T. (2003). Using decision trees to improve signature-based intrusion detection. Paper presented at the Recent Advances in Intrusion Detection.

46. Lee W and Stolfo. SJ. (2000). A framework for constructing features and models for intrusion detection systems. ACM Transactions on Information and System Security (TISSEC), 3(4), 227-261.

47. Li Xiao, Liu Y and Ni LM. (2005). Improving Unstructured Peer-to-Peer Systems by Adaptive Connection Establishment. IEEE Transactions on Computers, 54(9), 1091-1103.

48. Lui S, Lang KR and Kwok S. (2002). Participation incentive mechanisms in peer-to-peer subscription systems. Paper presented at the Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS'02).

49. Marina MK and Das SR. (2001). On-demand multipath distance vector routing in ad hoc networks.

50. McIlraith SA, Son TC and Zeng H. (2001). Semantic web services. IEEE Intelligent Systems, Special Issue on the Semantic Web, 16(2), 46-53.

51. Melby NJ. (2005). Comparative Relative Strength in Artificial Immune Systems: System Wellness.

52. Mills D, Martin J, Burbank J and Kasch W. (2010). Network time protocol version 4: protocol and algorithms specification. Internet Engineering Task Force, Tech. Rep. RFC, 5905.

53. Mirkovic J, Robinson M and Reiher P. (2003). Alliance formation for DDoS defense.

54. Oliveira LB, Siqueira IG and Loureiro AAF. (2005). On the performance of ad hoc routing protocols under a peer-to-peer application. Journal of Parallel and Distributed Computing, 65(11), 1337-1347.

55. Panagopoulos AD, Arapoglou PDM and Cottis PG. (2004). Satellite communications at Ku, Ka, and V bands: Propagation impairments and mitigation techniques. Communications Surveys & Tutorials, IEEE, 6(3), 2-14.

56. Parham P and Janeway CA. (2005). The immune system: Garland Science New York.

57. Roddy D. (1989). Satellite communications. New Jersey, Englewood Cliffs.

58. Roussopoulos M, Baker M, Rosenthal D, Guili T, Maniatis P and Mogul J. (2004). 2 P2P or Not 2 P2P? Paper presented at the The 3rd International Workshop on Peer-to-Peer Systems, San Diego, CA, USA.

59. Srour L, Kayssi A and Chehab A. (2006). Reputation-based algorithm for managing trust in file sharing networks.

60. Stepney S, Smith R, Timmis J and Tyrrell A. (1974). Towards a conceptual framework for artificial immune systems. Paper presented at the Proceeding of the 3rd International Conference on Artificial Immune Systems (ICARIS), LNCS 3239, 2004: 53-64. 28. teur), 125C.

61. Uddin M, Khowaja K and Rehman AA. (2010). Dynamic Multi Layer signature based IDS using Mobile Agents. International Journal of Network Security and its Applications, 2(4), 129-141.

62. Uddin M and Rahman AA. (2011). Reliability of Mobile Ad Hoc Networks through Performance Analysis of TCP Variants over AODV. Journal of Applied Sciences Research, 7(4), 437-446.

63. Uddin M, Rahman AA, Alarifi A, Talha M, Shah A, Iftikhar M and Zomaya A. (2012). Improving Performance of Mobile Ad hoc Networks using Efficient Tactical on demand Distance Vector (TAODV) Routing Algorithm. International Journal of Innovative Computing, Information and Control (IJICIC), 8(6), 4375-4389.

64. Wang C, Alqaralleh BA, Zhou BB, Till M and Zomaya AY. (2005). A blast service built on data indexed overlay network. Paper presented at the Proceedings of the First International Conference on e-Science and Grid Computing (E-SCIENCE '05), IEEE Computer Society, Washington, DC, USA.