ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (217-223), Month: April-June 2014, Available at: www.researchpublish.com

Study of P2P Networks Protection Opposing Malicious Attacks

R.Aruna[1], M.Narayanan[2]

[1]UG Scholar, [2]Assistant Professor
Department of Computer Science and Engineering
Saveetha School of Engineering
Saveetha University, Chennai, Tamil Nadu, India

Abstract: **P2P Network defined, any peer can connect and any peer can disappear the network without the permission of the server. So whatever peers are connecting to the network, they should protect always because many kind of peers are connecting to the web or internet. So this paper provides survey of P2P networks protection opposing malevolent attacks. Peer-to-Peer network is across this paper we will determine peer-to-peer networks, henceforth we will use the acronym P2P. A P2P network is a network that relies on computing exploitation of its clients slightly than in the network itself. We are investigating various P2P network attacks. This way the clients (peers) will do the fundamental procedures to retain the network going rather than a central server.**

Keywords: **Denial-Of-Service (DOS) Attacks, P2P network attacks, Worm Propagation, Man-in-the-middle Attack.**

1. INTRODUCTION

Peer-to-Peer Network is diagonally this paper determines peer-to-peer networks; henceforth we will use the acronym P2P. A P2P network is a network that relies on appending manipulation of its clients rather than in the network itself [1]. This way the clients (peers) will do the vital procedures to retain the network going rather than a central server. Progression, there are dissimilar stages of peer-to-peer networking [5]:

- **Hybrid P2P:** There is a central server that maintains data concerning the network. The peers are accountable for storing the information. If they wish to linkage one more peer, they query the server for the address.
- **Pure P2P:** There is absolutely no central server or router. All single peer performance as client and server at the alike instance. This is furthermore from time to time representing to as "server less" P2P.
- **Mixed P2P:** among "hybrid" and "pure" P2P networks. An instance of such a network is Gnutella that has no central server but clusters its peers regarding so-called "super-peers".

1.1 Historical

Although P2P networking has continued for rather a slight period, it has merely been admired currently and will reasonably be subject to even superior metamorphoses in the contiguous expectations. Napster was the early P2P demand that actually detained inedible. The technique it employment was fairly straightforward: a server indexed all the files each single user had. After a client inquired Napster for a file, the central server is supposed to respond beside a catalog of all indexed clients who by now owned the file. Napster-like networks are documented these days as early making networks. Such networks didn't have a complex implementation and frequently relied on a central server (hybrid P2P). The central server ideal makes sense for countless reasons: it is an effectual method to grasp hunts and permits to retain manipulation above the network. Although, it as well method there is a lonely position of breakdown.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (217-223), Month: April-June 2014, Available at: www.researchpublish.com

The formation networks are the novel mounting P2P networks. They are a respond to the legalized concentration P2P networks have been agreeable for insufficient years and have included ambiguity facial appearance. They have not up till now clutch the accumulation association major succeeding arrangement networks presently tolerate but this might change shortly. This P2P transformation clearly way enormous statistics of data will be accessible almost instantaneously to any peer for free [6].

This paper will nowadays be coordinated in 4 main sections [3]:

1. Primary, we will watch at innumerable vulnerabilities or attacks exposed in ended networks.
2. We will after that watch at extra detailed attacks particularly probable for P2P networks. Later these two scrutinies, we will endeavor to draw little near the beginning termination. We will next continue to our case study: Freenet.
3. To strength of mind systematically illustrates the Freenet construction.
4. Lastly, to determine effort to realize possible responsibility in Freenet and technique to improve them.

After this we will drawing our concluding conclusions and discover possible new instructions.

2. DENIAL-OF-SERVICE (DOS) ATTACKS

A Denial-Of-Service attack is do violence to on a computer or a network that reasons the overcome of ability [4]. In presence maintain innumerable forms or process to commit a DOS attack. In the container of P2P networks, the majority community form of a DOS attack is an endeavor to deluge the network alongside bogus packets, thereby bring to end justifiable network traffic. One more method is to sink the fatality in picky calculation so that it is too busy to do respond every additional query. DOS attacks are remote additional effective if more than a few hosts are encompassed in the attack, we after that coherent of a DDOS attack (Distributed Denial-Of-Service). Fig.1 shows that DOS attacks in P2P networks.

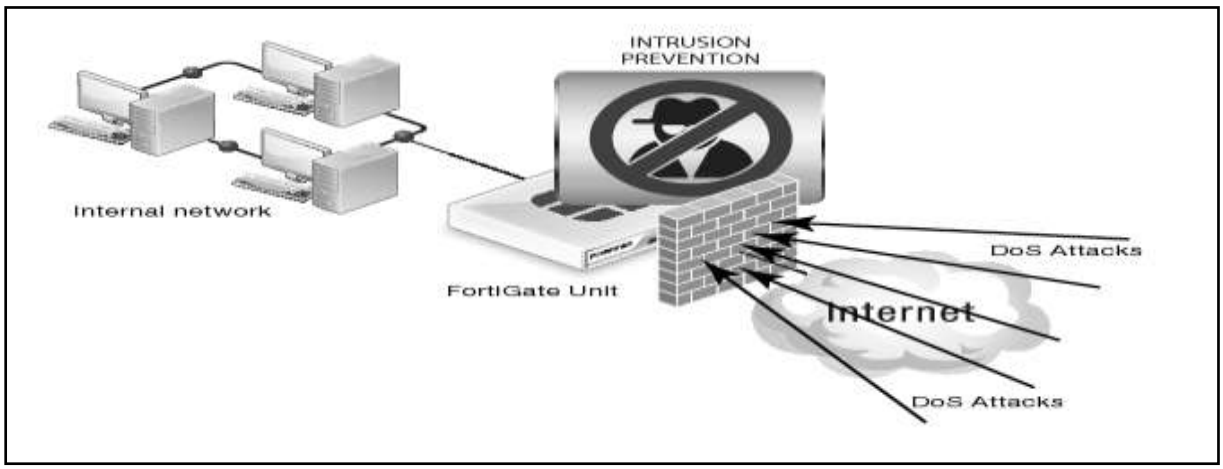

Fig.1: Diagram for Denial-Of-Service (DOS) Attacks

In a DDOS attack, the attacking computers are regularly classified computers beside broadband associations that have been compromised by a virus or Trojan. The performer can next distantly treatment these device (competent as zombies or slaves) and manage an attack at each host or network. To concludes, a DDOS attack can be even more amplified by employing uncompromised hosts as amplifiers. The zombies send off stress to the uncompromised hosts and send-up the zombies' IP addresses to the fatality IP. After the uncompromised hosts answer, they will dispatch the responding packets to the victim. This is recognized as a reflection attack.

2.1 Defenses

The earl y hold back is become conscious of a DOS attack as it can be mistaken beside a important utilization of the machine. DDOS attacks employing reflection are tremendously hard to chunk owing to the great numeral and variety of

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (217-223), Month: April-June 2014, Available at: www.researchpublish.com

mechanisms a malicious user can involve in the attack (almost every machine can be twisting into an automaton). In enhancement, as the attacker is frequently just circuitously included (he attacks crosswise the zombies and the thoughtful network), it is regularly unfeasible to distinguish [7].

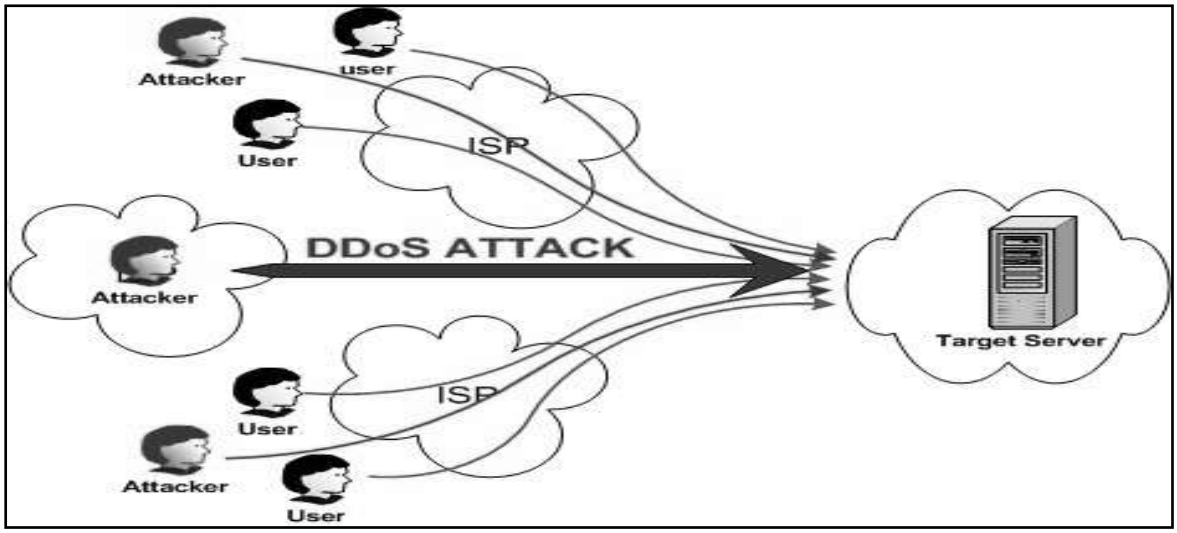

Fig.: 2: Diagram for DDoS Attacks

Fig.2: A DDOS attack: The attacker drive the arranges to the computers he just between you and me controls (masters) that next onward it to the zombies, that DOS as countless mechanisms as probable and spoof their IP to be the victim's, who will accord all the reply. Because of these feature, there survive no ended technique of overcrowding DOS attacks.
The congregation will there mystery to his clients earlier stand the require computation, consequently conservation that the clients go crossways an evenly comfortable totaling. DOS attacks are most effectual after the attacker consumes most of his victim's resources as spend tremendously inadequate resources himself. If every single endeavor to deluge his victim aftermath in him possessing to resolve a mystery beforehand, it becomes extra tough to raise a prosperous DOS attack. "Pricing" can be adjusted so that after the host perceives to be below an attack, it gives out extra luxurious puzzles, and consequently reduces the result of the attack.

2.2 Man-in-the-middle Attack

In a man-in-the-middle attack, the attacker put in himself unnoticed in the middle of two peers. Peer can after that choose to stay unobserved and secret agent on the contact or additional aggressively collision the announcement. Peer can achieve this by put in, tumbling or retransmitting preceding communication in the data stream [2].

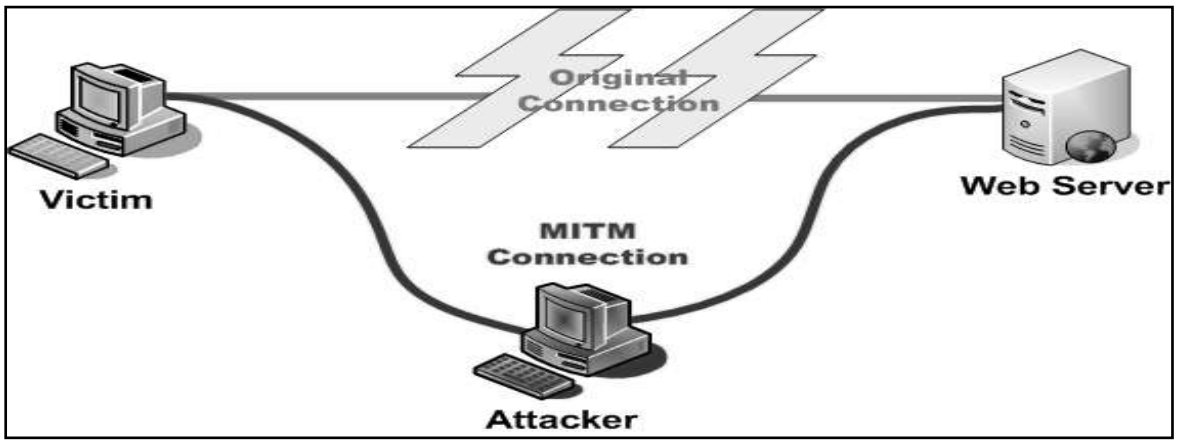

Fig.3: Man-in-the-middle attacks

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (217-223), Month: April-June 2014, Available at: www.researchpublish.com

Fig.3 shows Man-in-the-middle attacks. The Man-in-the-middle attacks can consequently complete a compilation of purposes, contingent on the protocol. In countless cases it is uniqueness spoofing or dispatch counterfeit in sequence. Man-in-the-middle attacks are a frightening in most protocols (particularly after there is a form of verification). Providentially, they are less attractive in P2P networks. All the peers have the alike "authorization" and the traffic's satisfied is public anyway that creates eccentricity spoofing ineffective. If the P2P request supports disparate clearances amid peers, next the implications of man-in the- middle attacks be supposed to depend on the protocol itself.

2.3 Worm Propagation

Fig.4 shows worm propagation in P2P networks. Worms by now pretense one of the largest menaces to the internet. At present, worms such as Program Red or Nimda are competent of contaminate hundreds of thousands of hosts within hours and no distrust that larger engineered worms should be bright to practically contaminate to seize the alike outcome in a material of seconds. Worms propagating diagonally P2P requirements must be disastrous: it is the weightiest intimidation.

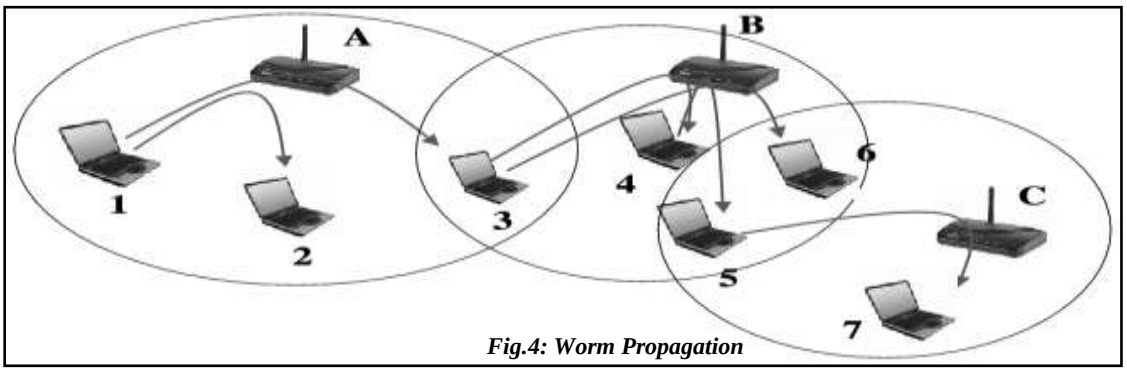

Fig.4: Worm Propagation

There are innumerable issues that create P2P networks attractive for worms [9]:

1. P2P networks are self-possessed by computers all management the alike software. Attackers can therefore cooperation the whole network by discovering merely one utilizable protection hole.
2. P2P peers predispose to interrelate along immeasurable dissimilar peers. Certainly a worm administration on the P2P apply for be supposed to no longer wobbly precious period scanning for complementary sufferers.
3. P2P wishes are consumed to transport enormous archives. Modest worms contain to ensure their capacity in regulate to clutch in one TCP packet.
4. The procedures are frequently not supposed as conventional and therefore harmony fewer thought from infringement uncovering systems.
5. P2P strategies recurrently run on classified computers somewhat than servers. It is consequently additional feasible for an attacker to have permission to susceptible records such as trust card numbers, passwords or address books.
6. P2P users repeatedly transmit unauthorized contented (copyrighted music, pornography ...) and could be less disposed to statement intermittent activities of the system.
7. The finishing and reasonably the majority succulent superiority P2P networks possess are their potentially enormous volume. After worms come to an end disseminate, their endeavor is usually to elevate great DDOS attacks.

2.4 Discovery Human Factor

The human factor should to forever be a consideration subsequent to security is at concern. We earlier saying that the upswing P2P desires have knowledgeable is furthermore due to ease of association and use, the low price (most of the period free of charge) and its exceptional rewards. Even beginner users have small complexity utilize such needs to download records that additional user's public deliberately or accidentally public on the P2P network.

This is so far one more protection setback P2P requests are posing. Enthusing a user, extraordinarily a learner, to make choices considering the convenience of their records is a important risk. Because of its suitable and acquainted stare, requirements such as Kazaa can cause a user to without knowing assign the contents of the papers or even worst, his

finished hard disk. Unfortunately, novice users do not comprehend the implications of their inaction alongside stare to security. Plainly closing the request for instance isn't plenty as most of them tolerate running in the background. Remarkably, millions of P2P peers are left running unattended and vulnerable for colossal eras of time. Malicious users alongside intermediate hacking skills can seize supremacy of such situations.

3. DESIGN OF SECURE P2P NETWORKS

Freenet is an improved unfasten foundation completion of the understanding define by Ian Clarke's July 1999 paper [8] and is categorized as a third formation P2P application. An early on version was released in March 2000. Freenet was conventional to react loneliness and potential setbacks subsequent creation requests at the moment practice. It was dexterity in sort to achieve pursuing 4 requirements:

- Anonymity for both creator and clients of in sequence.
- Deniability for stores of information.
- Resistance to activities of third social gathering to reject admission to information.
- Efficient animated storage space and routing of information

We will at the present time find out it in additional feature to distinguish how it supervises to come upon such supplies.

3.1 Proposing system Protocol Overview

Instinctively, Freenet can be apparent as a "chained" network. Like a link in a shackle, each single peer can merely converse beside it's manage neighbors. After a peer wants to query a file, it sends the memo to the most enthuse acquaintance, which wills in curl furthermore forward it to its most beat up support neighbor. After a memo is transmit, a peer has no method of determine out what will become obvious to it. It cannot inform to that peer the associate will in twist forward the memorandum to, or even whether the memo is undeviatingly reply by the associate itself. What's extra, a peer compliant a memo cannot notify if these memos originate from this associate or if it is merely forwarding a memo consented by a prior neighbor. This is the cornerstone supposed of the Freenet design that guarantees anonymity.

3.2 Proposing systems Protocol Details

A Freenet contract starts on at the side of a Request. Handclasp memorandum from one peer to one more, detail the necessary go back to address of the broadcast peer. If the distant peer is attentive and act in retort to stress, it will respond next to a Reply. Handshake detail the protocol edition number that it appreciates.

Handshakes are recalled for an insufficient hours, and consecutive deals amid the alike peers across this period could exclude this step. All memos include a randomly-generated 64-bit deal ID, a hops-to-live ensures, and a depth counter. Even though the ID cannot be definite to be exceptional, the likelihood of a come across transpiring across the deal lifetime amid the influence set of peers that it sees is extremely low.

3.3 Storing Data

Interleave pursue the comparable way as requirements. The user adjacent the commencing computes the confusion of the file and links its peer alongside the hash as well as a TTL. The peers will bypass on the "insert request" just as before. If the hops-to-live check is grasped missing a key encounter being observed, an "all clear" result will be range reverse to the basis inserter. The user subsequent sends the data, which is subsequent, show alongside the trail, familiarize by the adjacent the commencing query.

Every solitary peer alongside the pursue creates a new entrance in its direction-finding table subsequent to the inserter as data basis (although slight peers might select to select themselves or one extra peer as source). This mechanism has three belongings. First, at the moment interleave records are allocated on peers by nowadays owning analogous keys. This strengthens the clustering of keys instituted in the ask for apparatus. Second, inserts can be a mean to indicate the number present of new peers. Finally, attackers trying to displace ongoing files by locale in junk files below ongoing keys are probable to clearly choice the real files extra, as the innovative are show on rear-ender.

3.3.1 Management Data

Data is take hold of as an LRU (Least Currently Used), this method that in the draw to a close data can veto longer be obtainable on the network if all peers choose to plunge it. In this Freenet be different from supplementary arrangements (Eternity, Free Haven) that go behind to supply life span agreement for files.

3.3.2 Adding Peers

If have to be a protection stay if a new peer strength select his direction-finding key by himself. These regulations out the most forthright move toward. Later a peer relation to the web, it propels a petition alongside a particular TTL and sends it to a bordering peer. Every single solitary peer compliant such a petition computes an unintentional hash key and sends the petition to a random peer till the TTL is attained. All peers subsequent commit their hash key. All hashes are subsequent XORed and the significance is the new peer's hash. This yields a random key that cannot be exaggerated by a malicious contributor. Every single solitary peer subsequent adds an entrance for the new peer in its routing table below that key.

3.4 Attacks

As just seeming, Freenet seems flexible to innumerable attacks. The files are distributed across the web alongside tiny or no treatment from the clients, all data is encrypted and there tolerate living an authorizing instrument. Client cannot professionally check their connections that produce a incredibly influential nameless arrangement. In the conclude the file-request or file-insert queries are finished in a largely sensible manner, that prevents competent query-flooding DOS aggressions opposite the web (such as in Gnutella). Nonetheless, we will nowadays scrutinize insufficient probable attacks.

3.4.1 DOS Attack

The bulk forthright attack is to junk data storage. Its available two methods to understand these methods, whichever to demands the junk data from one additional malicious peer or undeviatingly interleave it in the network. Across the attack, the network is tremendously utilized to transfer the data and uploads the data. At presents excellent probability that balancing clients will undertake to download allocation of this unfeasible data and by substitute so, refuses period and bandwidth

3.4.2 The Malice and secret agent

If a peer unfortunately associates a hateful client to go in the web, subsequent the attacker can allocate him the span key he necessities (using this comparable accord, an attacker can select every single span keys he wishes as long as he is helped by complementary malicious peers). An attacker can manipulation a bordering peer to grasp opposing the regulation corporal by challenging it transversely him. As long as the attacker doesn't permit every single convoying peers across to the ineffective peer (only malicious ones), subsequent whatever this peer endeavors can be monitored. The attacker can use lexicon aggressions in order to decrypt all memos encrypted alongside KSKs that bypass across him (possible because in KSKs, the key is just a hash of a find string).

3.5 Anonymity

By looking at the TTL of the packets that go around crosswise the peer, a peer can increase apparition on how remote it is in the manacle of a accurate key. Even though Freenet from time to time arbitrarily increases the TTLs, this does not make them not feasible. For example if an attacker sends a request beside a TTL of 1 and be given a reply, next he can be pretty accurate that his associate is impressive the under attack file. He can moreover check how far period passes in advance the answer proceeds and use this data to make more inference. Finally, as define in proceed, an attacker can observe all data included in the packets bypassing across him. All this examine can give an attacker a good vision of the network surrounding him, yet this is not sufficient to totally split Freenet's anonymity.

Both peer can be related to each additional peer, as a result as quickly as a memo is bypassed on to a acquaintance, the attacker looses nearly all probable monitoring options. There is simply one case while an attacker can be sure that a peer is impressive a under attack file; if he has grasped to encircle the peer alongside malicious entities and doesn't discern each outgoing memos for an ingoing demand.

3.5.1 Simulation

In systematize to surround a conscientious confidence of that attacks are the majority effective opposite the Freenet construction, we selected to contain a simulation of the Freenet network. The peer's presentation is programmed in control to be as protected to a commonplace Freenet peer as attainable. They have manipulated storage space (50 files maximum), can merely link to a manipulated number of acquaintances and can disconnect from the web across the simulation run. Every solitary peer accepted at the origination countless files (25 in this container) chosen arbitrarily from a sphere records surrounding 20000 dissimilar archive who's keys be consistently dispersed. The network is accordingly brightly expertise athwart the main 10000 casual queries of every single solitary run of the reproduction, an initialization period we carry out not consider for the results. The reproduction is succeeding experienced for a complementary 1000 rounds diagonally that all consequences are examined. Memos were given a TTL of 30 hops and could be corrupted by malicious peers. The simulation was run innumerable period beside 3000 good peers and 30 malicious peers, the malicious peers visualize being superior diagonally the initialization stage. Previous to debating the consequences, we should to like to highlight the actuality that simulations cannot yet perfectly perfect realism though accurately they are put into operation. We resolve consequently not use the consequences undeviatingly other than additional to approach to be a faith of those attacks have to be most efficient.

4. CONCLUSION

Nowadays we are completed our study of protection in P2P networks. As a conclusion we can express the actuality to purely untainted P2P position a possibility disparate attacks, each category of shortcuts detained in the accomplishment can be twisting regarding in order to attack the P2P apply for in an extra treacherous approach. We in the closing stages distinguished that it be supposed to be fascinating for a PGP-like request to exist. This demand have to not purely apprehension pertaining to confirm client (binding area keys to substantial individuality) but moreover how remote confidence can be agreed to a region key. If such a request sustained, it might be exploit by P2P requirements as an enormously efficient fortification contrasting spiteful attacks.

REFERENCES

[1]. Scott Jensen: The P2P revolution peer-to-peer networking and the entertainment industry http://www.nonesuch.org/p2prevolution.pdf.

[2]. Lidong Zhou, Lintao Zhang, Frank McSherry, Nicole Immorlica, Manuel Costa, and Steve Chien: A First Look at Peer-to-Peer Worms: Threats and Defenses.

[3]. Jason E. Bailes, Gary F. Templeton: Managing P2P Security Considering the benefits and trade-offs of file-sharing systems.

[4]. D. Dumitriu, E. Knightly, A. Kuzmanovic, I. Stoica and W. Zwaenepoel: Denial-of-Service Resilience in Peer-to-Peer File Sharing Systems.

[5]. J. Liang, R. Kumar, Y. Xi, and K. Ross : Pollution in p2p file sharing systems In IEEE INFOCOM, 2005.

[6]. N. Christin, A. Weigend, and J. Chuang: Content availability, pollution and poisoning in peer-to-peer file sharing networks. In ACM E-Commerce Conference, 2005.

[7]. Thomas D¨ubendorfer, Arno Wagner: Past and Future Internet Disasters: DDoS attacks

[8]. RachnaDhamija: A Security Analysis of Freenet

[9]. Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron, Dan S. Wallach2: Secure routing for structured peer-to-peer overlay networks.