IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

A Confidential and Efficient Query in the Large Scale Attack

P. Jayalakshmi

, Department of Computer Applications, Urumu Dhanalakshmi College, Trichy-620019

Corresponding Author: jayababu07@gmail.com

Available online at: www.ijcseonline.org

***Abstract*--**YouTube, with large number of content creators, has turn into the ideal destination for watching videos online. Through the associate program, YouTube allows pleased creators to monetize their popular videos. Of significant consequence for content creators is which meta-level features (e.g. title, tag, thumbnail) are most receptive for promoting video status. The attractiveness of videos also depends on the social dynamics, i.e. the interface of the content creators (or channels) with YouTube users. The peer to peer (P2P) file distribution applications have owed a considerable amount of today's Internet traffic. Along with various P2P file sharing protocols, BitTorrent is the mainly widespread and trendy one that attracts monthly a quarter of a billion users from all over the world. Comparable to other P2P file sharing protocols, BitTorrent is frequently used for unlawful sharing of copyright protected files such as movies, music and TV series. To obstruct this enormous amount of illegal file distributions, anti-P2P companies have arisen to place against these applications (specially the BitTorrent). And our proposed approach Diffie Hellman algorithm ensures the secure transmission of data over a secure channel and enhances the performance of this proposed approach.

I. INTRODUCTION

In modern years, peer to peer (P2P) applications and protocols have been broadly extend all over the world and gained a significant reputation among Internet users. As declared, about 25% of overall Internet bandwidth is owed to the P2P traffic. Among all the P2P protocols, BitTorrent is the most eminent protocol, which is broadly used for sharing large files such as movies, music and TV series. presently, BitTorrent has 150 million instantaneous energetic users and about a quarter of a billion users monthly. This considerable amount of users contributes to additional than 17% of overall Internet bandwidth which obviously reveals the wonderful features of this P2P file sharing protocol. BitTorrent either can afford an economical and scalable technique for file distribution, as used by some not-for-profit software corporations (e.g. Eclipse and Linux), or can be used for downloading copyright secluded files, illegally. Since BitTorrent protocol and its client applications were not intended and urbanized by a single corporation, it is unfeasible to settle a lawsuit against them. Moreover, in most popular BitTorrent clients such as uTorrent, Vuze (Azureus) and FlashGet, Peer Discovery can be handled in a distributed manner without the existence of any centralized entity (i.e. tracker) which makes it even harder for copyright enforcement agencies to hamper BitTorrent lawfully. Unfortunately, nearly two-thirds of current BitTorrent traffic belongs to illegal sharing of copyright protected files such as music, movies or software. Accordingly, movies and music industries have started to hire anti-P2P companies to slow down the sharing of targeted music, movies and other products confined by copyright over P2P file sharing networks (i.e.BitTorrent). Those anti-P2P companies are attempting to advance the illegal distribution of copyright protected products using two different techniques: 1) Monitoring BitTorrent Networks; as affirmed in, there are some agencies (e.g. Media Defender), which as a result monitor BitTorrent networks, predominantly networks with trendy contents. By monitoring, they can send Digital Millennium Copyright Act (DMCA) make a note of notice to the end-users causal to sharing of copyright protected materials. As a confirmation of the liveliness of this technique, it is demand noting that most of the US universities have trustworthy rules about DMCA takedown notification traditional by college students. This is because of the escalating demand for barred music downloading among US college students. Unfortunately, it is possible to easily bypass the monitoring agencies without worrying about DMCA takedown notifications. For instance, as stated, there are some available IP block lists in order to preserve BitTorrent end users from establishing connection to anti-P2Pcompanies (e.g. Media Defender) or government related domains (e.g. DoD). In addition, numerous copyright holder agencies currently use inconclusive methods for identifying BitTorrent end-users contributing to illegal division of copyright protected files. The authors verified a simple practical technique for implicating innocent end-users in illicit content sharing. 2) Internet Attack Against BitTorrent Networks; Since Monitoring BitTorrent Networks cannot effectively stop end-users from downloading copyright protected content illegally, anti-P2P companies went outside just monitoring BitTorrent networks and attempted to begin attacks against them. There are various kinds of attacks

against BitTorrent networks based on the victim entity (such as attacks on lechers, seeders, peer discovery and torrent discovery). It was observed that the BitTorrent networks of top popular movies are under various kinds of attacks including Piece-Attack and Connection-Attack. However, according to the significant proportion of illegally traffic allocated by BitTorrent end-users, their results are not promising. Here, a question arises: "How can we get additional notable results from those attacks?" and consecutively "How much resources and equipment is necessary to have such a worthy outcome?" In this paper, we actively measure the effectiveness of Piece-Attack on BitTorrent networks. Piece-Attack is one of the attacks next to lechers in BitTorrent networks that were first observed against real torrent swarms. However the efficiency of the attack has not been actively deliberate yet. The contributions of this paper include: We dynamically measure the effectiveness of Piece Attack by launching it against different sort of real BitTorrent networks. We have fired large scale Piece-Attacks, via numerous public IP addresses used by hundreds of attacker peers. We frequent our measurements in several Scenarios to see the results of the attack against dissimilar kinds of BitTorrent networks. We point out the constraint factors that anti-P2P companies should consider in using this kind of attack against peers who contribute to public distribution of copyright protected materials in Bit-Torrent networks. To precisely measure the factors that can affect the intensity of Piece-Attack, in each scenario, we have ablaze lots of attacks with alternative number of public IP addresses used by our attacker peers and also varied number of attackers.

During these attack scenarios, we deliberate the amount of resources reserved by the attack to approximate the cost and the amount of resources needed for anti-P2P companies in order to significantly harass users who are downloading We show how anti-P2P companies can realize prominent results with a few possessions using this attack. To this finish, we have definite Attack Effectiveness, indicating how longer an subjective victim peer should linger in order to download a torrent file, completely. Attack efficacy is a useful factor for evaluating the success of the attack. We calculate it for each measurement to quantitatively determine the attack successfulness. We have also provided an analytical model in order to predict it with regard to the amount of resources allocated by the attackers. The model also can evaluate the amount of bandwidth mandatory for the attack. In other words, our model helps anti-P2P companies to analyze the attack's cost (i.e. number of attackers, number of public IP addresses and the amount of requisite data bandwidth) for a precise result. In order to launch plentiful numbers of attackers against a targeted BitTorrent network, we designed and urbanized an innovative Semi-Nat protocol in order to offer multiple IP addresses for torrent client applications, running on our attack host.

II. RELATED WORKS

[1] BitTorrent, each file is divided into pieces, where each piece is typically 256 KBytes. Each piece is further divided into blocks, with typically 16 blocks in a piece. When downloading a piece, a client requests different blocks for the piece from different peers. In the fake-block attack, the goal of the attacker is to prolong the download of a file at peers by wasting their download bandwidths. In particular, an attacker joins the swarm sharing the file by registering itself to the corresponding tracker. It then advertises that it has a large number of pieces of the file. Upon receiving this information, a victim peer sends a request to the attack peer for a block. The attacker, instead of sending the authentic block, sends a fake one. following downloading all the blocks in the piece (from the attack peer and from other caring peers), the victim peer performs a hash check diagonally the entire piece. The hash check then fails due to the fake chunk from the attacker. This requires the victim peer to download the entire piece (16 blocks) again, delaying the download of the file. If the peer chooses to download any of the blocks again from this or another fake-block attacker, the download is further delayed. letter that an assailant can cause a injured party look to waste 256 KBytes of download bandwidth by only sending it a 16 KByte block (using typical numbers). In this class of attacks, the attacker joins the targeted swarm and establishes TCP connections with many victim peers. Though, it never provide any block (authentic or fake) to its injured social gathering peers.

[2] A frequent version of this assail is the chatty peer attack. Here, the attack peer speaks the BitTorrent protocol with each of the victim peers, starting with the handshake message, and then followed by the bitmap message advertising that it has a number of pieces available for the file. When a victim peer requests one or more blocks, the attack peer doesn't upload the blocks. Moreover, the nature of the attacker is chatty. After the fatality peer sends one or more block requests, the attacker resends the handshake and bitmap messages. By resending these BitTorrent control mail above plus over again, the attacker persist as a neighbor, and the victim peer wastes a extensive time dealing with the attack peer, when it could have in its place downloaded blocks from other compassionate peers. The efficiency of this attack is enlarged if a momentous portion of victim's neighbors are unhelpful.

[3] A BitTorrent client is any program that outfits the BitTorrent protocol. Each client is able of preparing, requesting, and transmitting any type of computer file over a network, using the protocol. A peer is any computer running an example of a client. To split a file or group of files for further process, a peer first creates a tiny file called a

"torrent". This file contains metadata regarding the files to be communal and about the tracker, the computer that coordinates the file distribution. Peers that desire to download the file must first get hold of a torrent file for it and connect to the specified tracker, which tells them from which other peers to download the parts of the file. Though both eventually transfer files in excess of a network, a BitTorrent download differs from a classic download in numerous basic ways: BitTorrent makes various small data requests over dissimilar IP connections to different machines, while classic downloading is usually made via a single TCP connection to a single machine.

Architecture

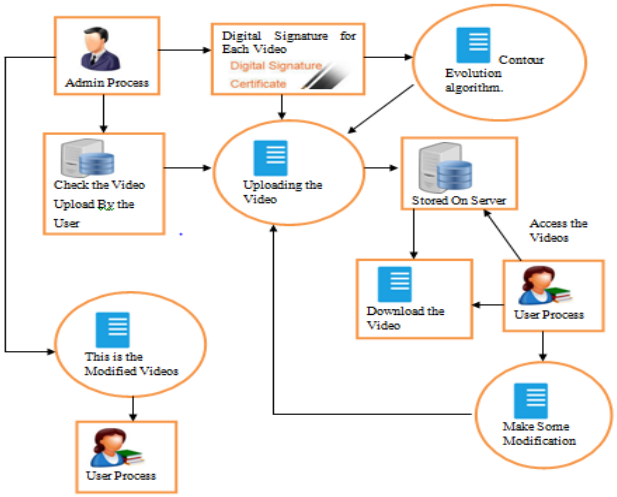

Fig1. Architecture

III. METHODOLOGY

Proposed Work

To exactly calculate the factors that can affect the strength of Piece-Attack, in each situation, we have ablaze lots of attacks with alternative numeral of public IP addresses used by our attacker peers and also varied number of attackers. Through these attack scenarios, measured the quantity of resources reticent by the attack to guess the cost and the amount of resources. And we advise a novel approach Diffie Hellman algorithm, provide secure transmission. Secure Transmission refers to the transfer of data such as private or proprietary information over a secure channel. A lot of secure transmission methods need a type of encryption. The most common email encryption is called PKI. In arrange to open the encrypted file an exchange of keys is done. Many infrastructures such as banks rely on secure transmission protocols to prevent a catastrophic break of security. Secure transmissions are set in place to avert attacks such as ARP spoofing and general data loss. Software and hardware in our system has been implemented to sense and prevent the illegal transmission of information from the computer systems to an association on the exterior may be referred to as Information Leak Detection and Prevention (ILDP), Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF) or Extrusion Prevention systems and are used in connection with additional methods to make certain secure transmission of data.

A digital signature is a mathematical method for representative the legitimacy of digital messages or documents. A legal digital signature gives a recipient cause to trust that the message was created by a known sender (authentication), that the sender cannot reject having sent the message (non-repudiation), and that the message was not distorted in transit (integrity). Digital signatures are a usual component of most cryptographic protocol suites, and are commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to spot forgery or tampering.

The digital corresponding of a handwritten name or stamped seal, but donation far more inbuilt sanctuary, a digital name is future to crack the problem of tampering and imposture in digital infrastructure. Digital signatures can offer the added assurances of facts to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Most recent email programs sustain the utilize of digital signatures and digital certificates, making it simple to sign any outgoing emails and validate digitally signed incoming messages. Digital signature is also used in general to give testimony of genuineness, data truthfulness and non-repudiation of haulage and transactions conduct over the Internet.

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind party to the communication. Equally, a digital name is a method that binds a person/entity to the digital data. This required can be in competition confirmed by receiver as well as any third party. Digital signature is a cryptographic value that is designed from the data and a secret key known only by the signer. In real world, the receiver of message desires declaration that the message belongs to the sender and he should not be able to disclaim the beginning of that message. This requirement is very critical in business applications, since likelihood of a dispute over exchanged data is very high.

IV. PERFORMANCE ANALYSIS

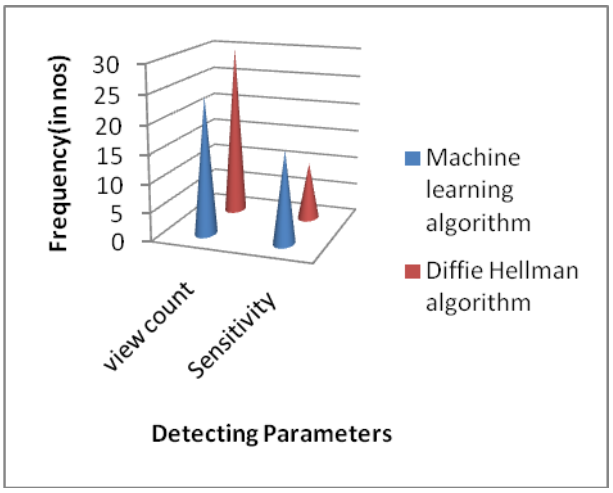

Figure.2

V. CONCLUSION

In this paper, we deliberate the impact of Piece-Attack on real BitTorrent networks. By initiation large-scale Piece-Attacks adjacent to numerous real BitTorrent networks, we pragmatic the success of the attack in prolonging the download time of end-users contributing to file sharing in the besieged networks. According to the results, we exposed that antiP2P companies can simply make the BitTorrent end-users to remain further than 10 times for downloading torrent files completely, only if they initiate the Piece Attack not after the Golden Period since the creation of the targeted swarm. We observed that even enormous amount of resources used by those companies cannot hamper the ability of BitTorrent protocol in public division of copyright confined contents and BitTorrent networks are entirely resilient beside Piece-Attack if they have approved their first month. As a prospect work, we propose to determine the blow of the Piece-Attack on BitTorrent networks for long term periods to figure out the opportunity of falling the adding up ratio of seeds in torrent swarms. Furthermore, we expect unusual networks to retort differently against the attack. Particularly non-quantitative parameters such as popularity or IMDB rating are good candidates to examine how various target movies oppose beside the Piece-Attack.

VI. FUTURE ENHANCEMENT

The kNN-R come near takes advantage of fast and protected RASP series query processing to implement kNN query processing. It knows how to position high exactness kNN results and also diminish the interactions between the cloud server and the in-house client. High precision kNNresults and minimized communications result in low in house workload. We have conducted a thorough security analysis on data confidentiality and query privacy. Compared to the related approaches, the kNN-R approach achieves a enhanced balance above the CPEL criteria.

REFERENCES

[1] (2014, March 16) An estimate of infringing use of the internet. [Online]. Available: http://documents.envisional.com/docs/Envisional-Internet Usage-Jan2011.pdf

[2] (2014, March 16) Google trends. [Online].Available:http://www.google.com/trends/explore#q=BitTorrent,kazaa,gnutella,edonkey,opennap&date=today%2012-m&cmpt=q

[3] (2014, Jan 5) BitTorrent. [Online]. Available: http://en.wikipedia.org/wiki/ Bit Torrent

[4] (2014, March 16) The eclipse foundation open source community website. [Online]. Available: http://eclipse.org

[5] (2014, March 16) Linux.org website. [Online]. Available: http://linux.org

[6] (2014, March 16) Comparison of BitTorrent clients. [Online]. Available: http://en.wikipedia.org/wiki/Comparison of BitTorrent clients

[7] P. Dhungel, D. Wu, and K. W. Ross, "*Measurement and mitigation of Bit Torrent leecher attacks*," Computer Communications, vol. 32, no. 17, pp. 1852–1861, 2009.

[8] G. Siganos, J. M. Pujol, and P. Rodriguez, "*Monitoring the BitTorrent monitors: A bird's eye view*," in Passive and Active Network Measurement. Springer, 2009, pp. 175–184.

[9] (2014, March 16) Media defenders official website.[Online].Available: http://www.mediadefender.com

[10] (2014, March 16) Copyright at mit. [Online].Available:http://web.mit.edu/copyright/dmca-notices.html

