An Active Measurement On Videos To Avert Deformation

Manoj Kumar[1] Assistant professor, V.S.Nirmala[2], J. Sapna Shilpi[3], P.Sharmili[4]
[1, 2, 3, 4] Dept of Information Technology
[1, 2, 3, 4] Saranathan College Of Engineering,Tiruchirappalli-620012,Tamil Nadu, India.

Abstract- *YouTube allows users to upload, view, rate, share, add to favorites, report, comment on videos, and subscribe to other users. It offers a wide variety of user generated and corporate media videos. Available content includes video clips, TV show clips, music videos, short and documentary films, audio recordings, movie trailers, live streams, and other content such as video blogging, short original videos and educational videos. YouTube offers users the ability to view its videos on webpages outside their website. Each YouTube video is accompanied by a piece of HTML that can be used to embed it on any page on the Web. The peer to peer (P2P) file distribution application shave 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.*

Keywords- Diffie Hellman algorithm, Bit Torrent, Digital Signatures, Secure Transmission.

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 theP2P protocols, BitTorrent is the most eminent protocol, which is broadly used for sharing large files such as movies, music and TV series. 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. Accordingly, movies and music industries have started to hire antiP2P 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. MediaDefender), 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 endusers causal to sharing of copyright protected materials.

As a confirmation of the liveliness of this technique, it is demand nothing that most of the US universities have trustworthy rules about DMCA take down 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 curr ently 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 movie s 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?"

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. 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.

II. METHODOLOGY

2.1. Existing Work

The study of popularity of YouTube videos based on meta-level features is a challenging problem given the diversity of users and content providers. Several models on characterizing the popularity of YouTube videos are parametric in form, where the view count time series is used to estimate the model parameters. The popularity of videos also depends on the social dynamics, i.e. the interaction of the content creators (or channels) with YouTube users. YouTube also has a social network layer on top of its media content to get popularity. Does not allow videos and view count dynamics which results from subscribers, migration. Due this popularity of YouTube channels will be low and interaction of users will not be good with the YouTube channels.

2.2. 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. 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 to as Information 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 can give a recipient cause to trust that he message was created by a known sender, that the sender cannot reject having sent the message , and that the message was not distorted during 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.

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.

2.3. System Architecture

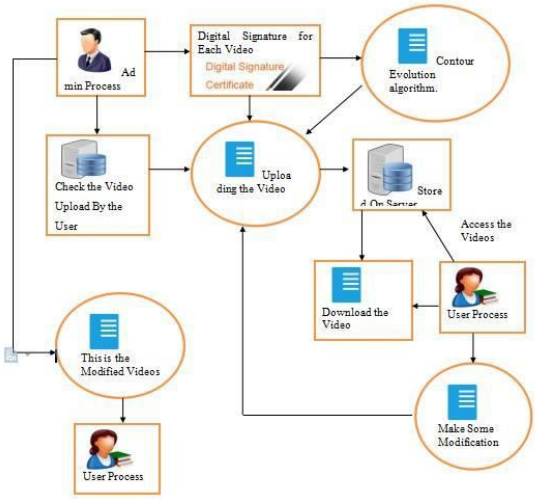

Fig 2.1: Architecture to Avert Deformation

2.4. MODULE SPECIFICATION

The projects contain several models are:

2.4.1 Server process (seeders)
2.4.2 Digital signature creation
2.4.3 Upload a video
2.4.4 Client process (leechers)
2.4.5 Apply transformation (piece of attacks)
2.4.6 Video tracking

2.4.1. SERVER PROCESS (SEEDERS)

In computing, a server is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client–server model, and a single overall computation is distributed across multiple processes or devices. Servers can provide various functionalities, often called "services", such as sharing data or resources among multiple clients, or performing computation for a client. A single server can serve multiple clients, and a single client can use multiple servers.

Fig 2.2: Server Process

2.4.2. DIGITAL SIGNATURE CREATION

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (nonrepudiation), and that the message was not altered in transit (integrity). Digital signatures are a standard element 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 detect forgery or tampering.

2.4.3. UPLOAD A VIDEO

Uploading videos to YouTube is a quick process either from your mobile device or from your computer. Follow this guide have your video online and attracting viewers in just a few minutes.

Fig 2.3: Uploading a video

2.4.4. CLIENT PROCESS (LEECHERS)

A client is a computer program that, as part of its operation, relies on sending a request to another computer program (which may or may not be located on another computer). For example, web browsers are clients that connect to web servers and retrieve web pages for display. Email clients retrieve email from mail servers. Online chat uses a variety of clients, which vary depending on the chat protocol being used. Multiplayer video games or online video games may run as a client on each computer.

Fig 2.4: Client Process

2.4.5. APPLY TRANSFORMATION (PIECE OF ATTACKS)

High quality conversion methods should also deal with many typical problems including:

Translucent objects Reflections Fuzzy semitransparent object borders – such as hair, fur, foreground out-of-focus objects, thin objects Film grain (real or artificial) and similar noise effects Scenes with fast erratic motion Small particles – rain, snow, explosions and so on.

2.4.6. VIDEO TRACKING

Video tracking is the process of locating a moving object (or multiple objects) over time using a camera. It has a variety of uses, some of which are: human-computer interaction, security and surveillance, video communication and compression, augmented reality, traffic control, medical imaging and video editing. Video tracking can be a time consuming process due to the amount of data that is contained in video. Adding further to the complexity is the possible need to use object recognition techniques for tracking, a challenging problem in its own right.

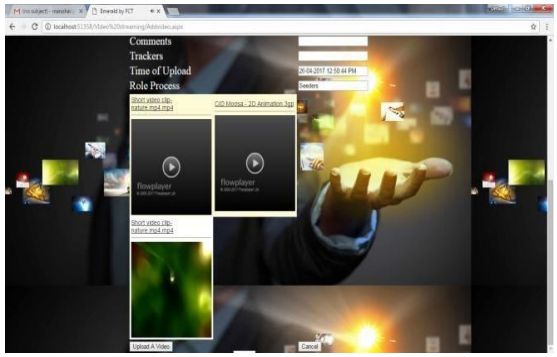

Fig 2.5: Video Tracking

2.5. ALGORITHM:

DIGITAL SIGNATURE ALGORITHM

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (nonrepudiation), and that the message was not altered in transit (integrity). Digital signatures are a standard element 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 detect forgery or tampering.

PSEUDOCODE

```
def generate_keys

# Gets random data and generates key pair end

def sign(message, secret_key)

#       Returns a signature of this particular message end

def verify(signed_message, public_key)

#       Returns `true' if signature can be verified, `false' otherwise

end

public_key, secret_key = generate_keys real_signature = sign("Video", secret_key)
fake_signature = sign("Sample", "random string")

verify(real_signature, public_key) # Returns true

verify(fake_signature, public_key) # Returns false .
```

III. RELATED WORKS

3.1. An estimate of infringing use of the internet.

BitTorrent, each file is divided into pieces, where each piece is typically 256 Kbytes. Each piece is further divided into blocks, with typically 16Kbytes 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. Downloading all the blocks in the piece the victim peer performs a hash check for entire piece of file. The hash check, 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 the middle of attacks, the attacker joins with the targeted swarm and provides TCP connections with many of the victim peers. Though, it never provide any block

(authentic or fake) to its injured social gathering peers.

3.2. Google trends and the forecasting performance of exchange rate models

A frequent version of this assail is the chatty peer attack. Here, the attack peer communicates the BitTorrent protocol with all of the victim peers, beginning with the handshake message, and then followed by the bitmap message advertising that it has a number of pieces available for the particular 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 the Bit Torrent mail over again, the attacker act as a peer, and the victim peer wastes an extensive time dealing with the attack peer, whereas it could have been done by its place downloaded easily. The efficiency of this attack is enlarged if a momentous portion of victim's neighbors are unhelpful.

3.3. The BitTorrent P2P file-sharing system:

Measurements and Analysis

A Bit Torrent client is a program that outfits the Bit Torrents protocol. Each client can make request and transmit any type of computer file over the network, using this protocol. To split a file or group offiles 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.

IV. 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 PieceAttack 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.

V. 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 kNN results 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 approach achieves a enhanced balance above the CPEL criteria.

REFERENCES

[1] (2014, March 16) An estimate of infringing use of the internet .
[2] (2014, March 16) Google trends and the forecasting performance of exchange rate models.
[3] (2014, Jan 5 The BitTorrent P2P file-sharing system: Measurements and Analysis.