Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Stegtorrent Using Data De-Clustering

Murkute Reshma, Pattiwar Nikita, Shere Shalaka, Thombare Nalini
Student,Department of Information Technology, MMIT,
Lohgaon, Pune, Maharashtra, India

Abstract: Nowadays, people widely use internet for data uploading and downloading using torrent.Previoussystem was less secure and time consusming. To overcome this problem we are going to implement stegtorrent using data de-clustering StegTorrent a new network steganographic method for file transfer service.Availability and scalability of storage systems are vital for existing information systems. Many applications require considerable space, which is increasing rapidly, and essential data kept in storage must be retained. To satisfy these requirements, parallel storage configurations with multiple disk drives are commonly adopted. For these, data placement methods are critical in realizing high availability and scalability. When one copy is damaged by a disk failure, the other can continue to be used.It is also important to lower the cost of update operations in the replication-based approach. For better space utilization, and greater scalability it is important. To ensure that the data mapping and requests are evenly divided among disks. It has the advantages of low cost data modification and data recovery of the replication-based approach and the advantages of query filtering and the clustering effect from the value range partitioning.

Keywords: Network steganography, Bittorrent , information hiding, Clustering and De-clustering, Partitioning, Disk Failures, StegTorrent.

I. INTRODUCTION

Availabilityand scalability of storage systems are vital for existing information systems. Manyapplications require rapidly increasing considerable space, and essential data must be retained. To satisfy these requirements, parallel storage configurations with multiple disk drives are commonly adopted. For these, data placement methods are critical in realizing high availability and scalability.One approach to achieving high availability of parallel disk systems is to replicate the data items on separate disk drives. When one copy is damaged by a disk failure, we can use continue . till both copies are corrupted at the same time, the single disk failure will be transparent to applications, and service will not be interrupted. For example the chained de-clustering is a well-known parallel data placement method using replicas. For many applications horizontal data partitioning is commonly used. The horizontal partitioning strategies fall into three types: round-robin, hash and value-range partitioning. The value-range partitioning can efficiently treat range queries as well as exact match queries. Moreover, clustering effect of the partitioning, which stores continuous data into physically neighbouring disk pages, for many applications provide better performance. However, the skews may generate by value range partitioning during repeated updates. The round-robin partitioning produces no skew but is ineffective for queries because it requires brute-force searches.The hash partitioning provides good performance for exact match queries and produces relatively little data skew, but is ineffective for range queries because it randomizes the data location, which means that the clustering cannot occur using the hash partitioning. Therefore partitioning strategies have advantages and disadvantages. However, the disadvantage of the value-range partitioning can be reduced if the data allocation and range criteria can be modified dynamically. The data skews caused by repeated update can bealtered by migrating data between disks.

II. RELATED WORK

BitTorrent is one of the few that has managed to attract millions of users. For searching the file Bittorrent uses global component. To know more about the In bittorent, we focuses on Availability , integrity and download performance. To aid in the understanding of a real P2P system that apparently has the right mechanisms to attract a large user community.

For file-downloading, Bittorrent is one of the protocol. In BitTorrent, files are divided into different parts, and to prevent parasitic behaviour the *downloaders* of a file *barter* for chunks of it by uploading and downloading them in a tit-for-tat-like manner. Each peer is responsible for maximizing its own contacting suitable peers, and peers with high upload rates will with high probability also be able to download with high speeds.

Steganography has been previously research, by research community in p2p network. Information hiding techniques were also be used. Following we are discussing some of the techniques in which steganography is used:-

2.1. Mnemosyne: Peer-to-Peer Steganographic Storage

For creating steganographic storage service like Mnemosyne [1] which is local storage system to be distributed on p2p system. Mnemosyne advantage is low cost in network bandwidth and disk space is also less. In this system, server

contains unreliable storage block. And functions of node can serve on both server and client side simultaneously. A steganographic method is used in existing p2p system.

2.2A Steganography Scheme in P2P Network

As compared to bittorrent specific steganographic method [2] steganography scheme in p2p network uses bittorrent and torrent file. This file format is run on internet.[3] It consist of two approaches, changing the letter case in url which is known as letter case change(lcc)and another is reuse of torrent file called field re-usage. This produces stegtorrent. But it is less secure to insensitivity of data hiding and other is reuse of torrent file may spoil the embedded information.

2.3. The Steganographic File System

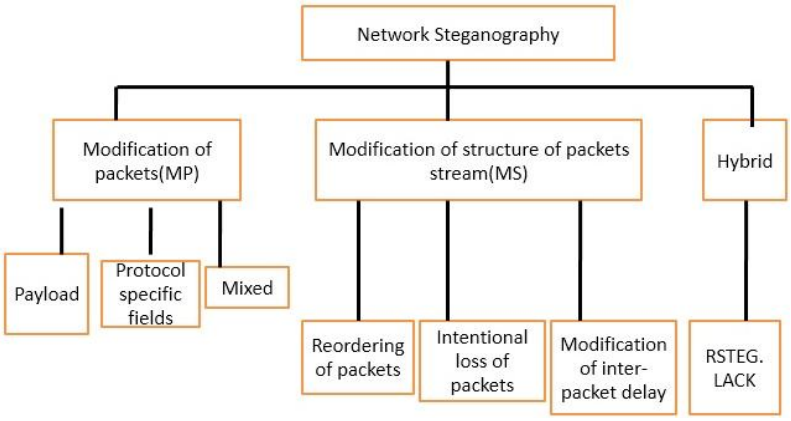
In steganographic file system has high level of protection, because those who knows name and password only can access the file but attacker can try various types of password to get data. The main purpose of bitthief is to merge data from bittorrent for free riding.

2.4. Hidden Communication in P2P Networks Steganographic Handshake and Broadcast

In hidden communication p2p network for file sharing. It is publicly available in steganographic handshake. It consist of bittorent client and bitthief Our proposed system contains steganographic methods that applies to bittorrent called as stegtorrent. .Bitthief has only downloaded file without uploading this contains spoiling of data. To avoid this it uses tit-for-tat protocol.For this to enable hidden communication fragement request must vary in terms of sequence. In this paper data and time are divided into fragements. Therefore it has low steganographic bandwidth, because it set the port for hidden communication. This method did not provide any experimental result as they are not evaluated properly.

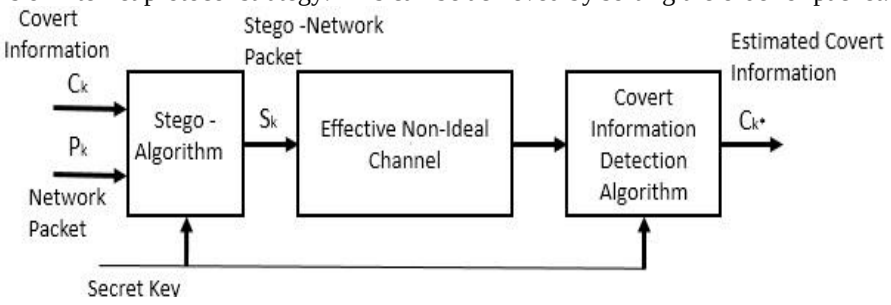
2.5. Retransmission Steganography and Its Detection

[5]This system modifies the order of packet and there are many methods to modify the timing relation between PDU (protocol data units), to introduce steganographic method for retransmission steganography. The main aim of retransmission steganography is to receive the order of packet. The modification may replaces the data. For ordering of packet PDU is used .PDU affects on modification of the data with their time and may get lost. Retransmission mechanism is used which is based on time-out .It tells the receiver that to acknowledgement for each received packet. If packet is sent successfully then acknowledgement is sent. If packet is not received then send it again. The RSTEG can be used to exchange steganogram .In this method, both sender and receiver knows the steganographic method. During connection they send the packets to each other. If receiver is not receive the packet sender must require to retransmit the packet. To avoid retransmission of packets sender again replaces the original payload of packet with steganogram. When receiver receives the retransmissions packets, it extract the hidden information. By using sequence number field from IPSEC protocol header this reordering of packet can be achieve.



2.6. Practical Internet Steganography: Data Hiding in IP

[6]For ordering of packet we introduce a new practical internet steganapgraphy for data hiding in IP. In this paper hiding of data in internet using steganography. Data hiding scenario is more practical and robust because they are based on duplications of internet protocol strategy. This can be achieved by sorting the order of packet.

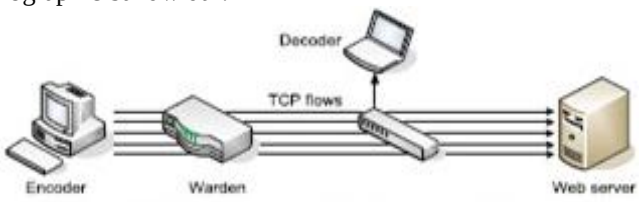


2.7. Steganographic Communication In Ordered Channel

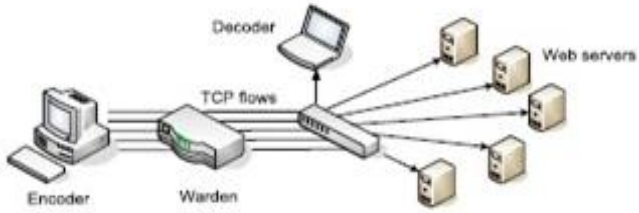
To avoid this [7], we introduce steganographic communication in ordered channel. In this paper whatever the information is embedded in packet sequence ,in terms of ordered channel. This may coz packet loss .To improve this new techniques are used. All these methods are lacking because of detetactability. And steganographic bandwidth. In IP network ordering is an one side transmission. When the order of packet is exploited .It may easy to recover. For that it requires synchronisation mechanism to extract secret data.

2.8. Robust Network Covert Communications Based on TCP

To achieve this synchronization mechanism lower bandwidth.[8] we proposed robust network communication in TCP.When receiver is receiving the data,the data will be in hidden form.To achieve this,it requires transmitter-receiver synchronization,for extraction it requires steganography.To improve,our proposed system stegtorrent using data decclustering we are using bittorrent one-to-many transmission and packet number and their order is in sequence therefore it contains high steganographic bandwidth.



(a) Five TCP flows connect to the same Web server.



(b) Five TCP flows connect to different Web servers.

Two covert communication scenarios for Cloak.

III. CONCLUSION

Due to lack of security related to data sharing in existing system, We are going to propose this system 'StegTorrent using data de-clustering' with the help of Steganography .This project helps users to upload/download files with more speed and securely. If any third party user trying to catch the data he will not get whole data from one server. The data which he get will be in the hidden form. So, it will not be easy to hack information.

This project helps for organization, As the demands for highly secure and high speed data increasing rapidly.

ACKNOWLEDGMENT

We would like to thank the entire department of Information Technology Engineering for their sincere guidance and continuous motivation and support to gain superior degree of knowledge in the vast domain of Information Technology. We are very thankful to our project guide who supported us and guided us to implement this project with great success. Also thankful to all teachers who motivated us to achieve this goal.

REFERENCES

[1] S.Hand, T.Roscoe,"Mnemosyne:Peer-to-Peer Steganographic Storage",Proc. of IPTPS 2002,LNCS 2429,PP.130-140,2002.

[2] Zishuai Li, Xingming Sun, Baowei Wang, Xiaoliang Wang, "A Steganography Scheme in P2P Network," Proc. of InternationalConference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2008), August 2008, pp. 20–24.

[3] R. Anderson, R. Needham, A. Shamir. "The Steganographic File System," Proc. of International Workshop on Information Hiding, 1998.

[4] R. Eidenbenz, T. Lechery, R. Wattenhofer, "Hidden Communication in P2P Networks Steganographic Handshake and Broadcast," Proc. of IEEE INFOCOM 2011, April 2011, pp. 954–962.

[5] W. Mazurczyk, M. Smolarczyk, K. Szczypiorski, "Retransmission Steganography and Its Detection," Soft Computing, Vol. 15, Issue 3,pp. 505–515, 2011.

[6] D. Kundur, K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Workshop on Security of InformationSystems, College Station, Texas, 2003.

[7] R. C. Chakinala, A. Kumarasubramanian, R. Manokaran, G. Noubir, U. Rangan, R. Sundaram, "Steganographic Communication inOrdered Channels ," Proc. of Information Hiding (IH2006), LNCS, 2006.

[8] X. Luo, E. Chan, P. Zhou, R. Chang, "Robust Network Covert Communications Based on TCP and Enumerative Combinatorics,"IEEE Trans. Dependable Sec. Compute. 9(6): 890-902 (2012)

