Computer Networks 79 (2015) 39–52

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Fighting pollution attacks in P2P streaming

Md. Tauhiduzzaman, Mea Wang *

Department of Computer Science, University of Calgary, Canada

ARTICLE INFO

Article history:
Received 17 July 2013
Received in revised form 5 October 2014
Accepted 17 December 2014
Available online 6 January 2015

Keywords:
Peer-to-Peer
Multimedia streaming
Pollution attack
Reputation system

ABSTRACT

In recent years, the demand for multimedia streaming over the Internet is soaring. Due to the lack of a centralized point of administration, Peer-to-Peer (P2P) streaming systems are vulnerable to pollution attacks, in which video segments might be altered by any peer before being shared. Among existing proposals, reputation-based defense mechanisms are the most effective and practical solutions. We performed a measurement study on the effectiveness of this class of solutions. We implemented a framework that allows us to simulate different variations of the reputation rating systems, from the centralized global approaches to the decentralized local approaches, under different parameter settings and pollution models. One key finding is that a centralized reputation system is only effective in static network and in defending against light pollution attacks. In general, a fully distributed reputation system is more suitable for the "real-time" P2P streaming system, since it is better in handling network dynamics and fast in detecting the polluters. Based on this key finding, we propose DRank, a fully distributed rank-based reputation system. Experimental results show that this technique is more flexible and robust in fighting pollution attacks.

1. Introduction

In recent years, the demand for multimedia streaming over the Internet is soaring. The distribution of multimedia contents requires a large amount of resources. For example, broadcasting videos in YouTube [1] costs Google millions of dollars per day to maintain the server space and upload bandwidth. To better accommodate the large demand and to increase the scalability of the service, the Peer-to-Peer (P2P) infrastructure is a good alternative for multimedia streaming. P2P streaming systems, *e.g.*, BBC iPlayer [2], PPLive [3] and UUSee [4], have been widely deployed to serve millions of users around the world. In a P2P live streaming system, at the source, the streaming file is divided into small *segments* representing a short duration in the video playback. The segments are then sent into the network and are shared among peers in the system. Compare to conventional client–server approach, P2P streaming alleviates the workload on the content source by inviting peers to contribute their bandwidth. However, due to the lack of a centralized administrative point, the segments might be altered by any peer before being shared. The system is under a *pollution attack* if unauthorized or unauthenticated information is inserted into the segments by one or more peers in the system.

Pollution attack in P2P file-sharing systems [5] is normally launched by copyright holders to fight copyright infringements. The same motivation works behind this attack in the P2P streaming systems, as experimented in [6]. Although this motivation makes this attack legal, the idea can be used illegally. Competing broadcasting companies can try to sabotage each other using pollution attack, or malicious users can launch this attack just as a prank. This attack can even be launched unintentionally by poorly

* Corresponding author.
E-mail addresses: mtauhidu@ucalgary.ca (Md. Tauhiduzzaman), meawang@ucalgary.ca (M. Wang).

http://dx.doi.org/10.1016/j.comnet.2014.12.009
1389-1286/

configured software. Regardless of the motivation, pollution attack can be severe enough to make the entire system collapse with very little effort from the attacker.

According to [5], a pollution attack is a simple but effective method to degrade the P2P system performance. In the KaZaA file sharing system, there may be 8000–50,000 polluted versions of a single file in the entire network. According to [7], in file sharing systems like KaZaA, eDonkey and Gnutella, a small amount of polluted content can easily cause scarcity of the files. Polluters can also increase the severity of the attack by simply adding a few versions of a file to the network, even if they have very limited bandwidth [8]. A malicious peer, referred to as a *polluter* herein, can inject polluted content either aggressively or non-aggressively. A non-aggressive polluter downloads content as a regular peer and alters the content before sharing with others, whereas an aggressive polluter lures peers by simply advertising that it has all segments. While watching the video, viewers see either altered content or completely different video frames, leading to discontinuations of the regular playback or unexpected video content. As shown in [9,10], the entire network can be infected even by a single polluter in less than a minute.

To fight pollution attacks in such a distributed system, many reputation-based defense mechanisms have been propose. In its simplest application, peers rate their neighbors' reputation and stream segments from neighbors with good reputation. The reputation system has a wide range of applications in P2P and distributed systems, including trust management, system auditing, incentive building, and defense mechanisms. In order to gain an deeper understanding of the effectiveness of the reputation-based defense mechanisms against pollution attacks, instead of evaluating and comparing different proposals, we studied two key steps in fighting against pollution attacks. The first step is collecting and compiling peer reputations. We explored different collection methods and their accuracy under different pollution models. The second step is identifying and isolating polluters. We examined strategies for isolating polluters in a P2P streaming system. The results of this study is summarized in [11] and recapped in Section 3.

The analysis presented in [11] identified the advantages and limitations of different reputation approaches. One key finding is that a centralized reputation system is only effective in static network and in defending against light pollution attacks. In general, a fully distributed reputation system is more suitable for the "real-time" P2P streaming system, since it is better in handling network dynamics and fast in detecting the polluters. Based on this key finding, we propose *DRank* in this paper. DRank is a fully distributed rank-based reputation system. Experimental results show that this technique is more flexible and robust in fighting against pollution attacks.

The rest of the paper is organized as follows. We discuss existing defenses against pollution attacks in P2P live streaming systems in Section 2. Section 3 provides background information on P2P streaming and pollution attacks, and recaps the key findings in [11] to motivate the new proposal. Based on the key findings, we propose DRank, a new reputation-based defense mechanism to fight pollution attacks, in Section 4, followed by the performance evaluation in Section 5. Finally, in Section 6, we conclude our work.

2. Related work

The spreading of the polluted segments not only degrades the video quality, but also helps spread viruses, bots, and malware. Because of the anonymous and dynamic nature of the P2P infrastructure, it is difficult to identify the polluters. Polluters exploit the innocence of peers to distribute polluted segments widely. This also makes it difficult for the defense mechanisms to distinguish the polluters from victim peers. Expelling an innocent peer will harm the streaming quality as the system not only loses bandwidth supply, but also good peers that can serve clean segments. In addition, the polluters may use intelligent approaches, *e.g.*, whitewashing and collusion attacks against any defense mechanism being applied. In a *whitewashing attack*, a malicious peer tries to improve its image by changing its identity [12] or showing occasional good behavior (on–off attack) [13]. In a *collusion attack*, a set of polluters collaboratively rank each other high and rank regular peers low in order to confuse the ranking system. These additional attack strategies make the pollution attack a burning issue [14].

To defend against pollution attacks in P2P systems, several approaches have been proposed in the past years. The approaches are best summarized in three categories: cryptographic approaches, blacklisting, and reputation systems. The cryptographic approaches employee hashing mechanisms and distributed verification techniques to identify polluted content as well as the source of the pollution [5,9,15]. Liang et al. [5] proposed a fingerprint verification technique, in which each segment of a shared file is imprinted with a fingerprint by the origin peer. The fingerprints is then checked against a trusted database created by the source. Furthermore, Dhungel et al. [9] present several cryptographic approaches, including traffic encryption (verification and chunk signing techniques) hash verifications (integrity checking). Although these techniques can be applied in either a centralized way or a decentralized way, they require intensive computation either on the source server or among peers in the network. In a P2P streaming sessions, video segments are being rendered by the video players as they are being received. It is a real challenge to deliver and verify the fingerprints and hash values in such a real-time system. For this kind of defense, a peer must trust the disseminators of the hash code [16]. However, a disseminator could also be a malicious peer trying to provide the matching hash code for polluted segments.

In contrast to the cryptographic approaches, blacklisting [9,17] is easy to implement and is very effective for straightforward pollution attacks. In such a system, peers monitors each other and reports any malicious behavior. Peers exhibiting malicious behavior are blacklisted and avoided by regular peers. Although this technique can effectively isolate the polluters in the system, to counteract it, a polluter may combine a whitewashing attack or a collusion attack with the pollution attack.