Computer Networks 72 (2014) 62–73

Contents lists available at ScienceDirect

Computer Networks

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

A trust-based pollution attack prevention scheme in peer-to-peer streaming networks ☆

Xin Kang *, Yongdong Wu

Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, Singapore 138632, Singapore

ARTICLE INFO

Article history:
Received 4 December 2013
Received in revised form 5 June 2014
Accepted 23 July 2014
Available online 4 August 2014

Keywords:
Peer-to-peer networks
Pollution attack
Trust management
Multimedia streaming

ABSTRACT

Nowadays, peer-to-peer (P2P) streaming systems have become a popular way to deliver multimedia content over the internet due to their low bandwidth requirement, high video streaming quality, and flexibility. However, P2P streaming systems are vulnerable to various attacks, especially pollution attacks, due to their distributed and dynamically changing infrastructure. In this paper, by exploring the features of various pollution attacks, we propose a trust management system tailored for P2P streaming systems. Both direct trust and indirect trust are taken into consideration when designing the trust management system. A new direct trust model is proposed. A dynamic confidence factor that can dynamically adjust the weight of direct and indirect trust in computing the trust is also proposed and studied. A novel double-threshold trust utilization scheme is given. It is shown that the proposed trust management system is effective in identifying polluters and preventing them from further sharing of polluted data chunks.

1. Introduction

1.1. Background and motivation

The past decade has witnessed the rising of large-scale multimedia social networks, over which millions of users interact with each other and exchange media contents in a distributed way. Among all the multimedia social network applications, peer-to-peer (P2P) streaming is popular and successful due to its high scalability, robustness, and satisfactory performance. Currently, there are two categories of P2P streaming systems: *tree-based* [2,3] and *mesh-based* [4,5]. In tree-based P2P streaming systems, the media content is encoded and divided into small chunks by a root node, and is then distributed to his children nodes. Then, these children nodes forward the received chunks to their children nodes. The data chunks are not forwarded any further at the leaf nodes which reside at the bottom of the tree. In mesh-based P2P streaming systems, the media content is encoded and divided into small chunks by peers. Each peer maintains a buffer map announcing available and desirable chunks. Peers exchange their buffer maps, and then upload or download data chunks according to their interests. Unlike the tree-based systems, mesh-based systems do not need to build and maintain a fixed streaming topology, and thus overcomes the bandwidth bottleneck problems existing in tree-based streaming systems. Today's most popular P2P streaming applications, such as PPTV [6], PPStream [7], and SopCast [8], are all mesh-based streaming systems.

In these P2P streaming networks, peers are assumed to be well behaved and non-malicious. To the best of our knowledge, few of them are designed to be resistant to pollution attacks. However, due to their distributed and dynamically changing infrastructure, P2P streaming

☆ Part of this work has been presented in IFIP SEC 2012 [1].

* Corresponding author.
E-mail addresses: xkang@i2r.a-star.edu.sg (X. Kang), wydong@i2r.a-star.edu.sg (Y. Wu).

http://dx.doi.org/10.1016/j.comnet.2014.07.012
1389-1286/

systems are vulnerable to various attacks, especially pollution attacks. Malicious peers may intentionally forge data chunks or alter received data chunks, and make these polluted data chunks available to other peers. Without the ability to differentiate between malicious peers and good peers, peers are highly likely to request and forward polluted data chunks, consequently degrading the performance of the whole system. Therefore, effective pollution-resistant mechanisms are badly needed for P2P streaming systems.

1.2. Related work

A number of scholarly work has been published in literature on the design of pollution-resistant mechanisms for P2P streaming systems. In [9], by measuring the PPTV streaming system, the authors showed that without any pollution-resistant mechanisms, the polluted content could spread through much of the P2P network. Then, the authors proposed four possible defenses to pollution attack, namely, blacklisting, traffic encryption, hash verification, and chunk signing. In [10], the authors presented a framework to secure P2P media streaming systems from malicious peers by utilizing a subset of trusted peers to monitor the bandwidth usage of untrusted peers and throttle the malicious peers in the system. In [11], the authors investigated the scenario that polluters could upload polluted and clean chunks alternatively to avoid being detected, and a trust management system was then proposed to defend this kind of pollution attacks.

On the other hand, trust management mechanisms have been extensively studied in literature for a wide range of applications, such as electronics commerce [12–14], ad hoc networks [15–17], P2P networks [18–29]. However, trust is in nature a complex psychological concept involving a lot of complex properties, such as uncertainty, fuzziness, asymmetry, and time attenuation. The methodology used to model the trust has a significant influence on the performance of the trust management system. Trust models should be tailored to meet the specific requirements of different P2P applications. In this paper, by exploiting the unique features of pollution attacks, we design a trust management system to defend against various types of pollution attacks for P2P multimedia streaming systems. Two closely-related work are [23,27]. In [23], the authors developed a fully distributed trust management system named as PeerTrust. PeerTrust adopts the public-key infrastructure for securing trust scores and uses overlay for trust propagation. In [27], the authors proposed PowerTrust, which is a robust and scalable P2P reputation system. They leverage the power-law feedback characteristics to build up a distributed reputation ranking system. PowerTrust can help peers to identify the most reputable peers quickly and accurately. However, both PeerTrust and PowerTrust adopt a fixed weight factor to balance the weight of direct and indirect trust, and use a single-threshold approach to identify dishonest peers. Most importantly, the trust models and the trust updates schemes adopted in PeerTrust and PowerTrust are not tailored to fighting against pollution attacks.

1.3. Main contributions

The main contributions of this paper are listed as follows:

- A theoretic framework on the modeling of trust management systems to fight against pollution attack in P2P streaming systems is proposed and investigated.
- A dynamic confidence factor is proposed to dynamically adjust the weight of direct and indirect trust in computing the trust, which is shown to be pretty effective in reducing the negative effects of the bad-mouthing attack and the collusion attack. Guidelines on how to deign such a dynamic confidence factor are given, and two specific designs of the dynamic confidence factor are proposed and investigated.
- A novel approach to model the direct trust is proposed based on the unique features of pollution attacks. It is rigorously proved that the proposed trust model is effective in defending against the on–off pollution attack introduced in Section 4.3.
- A novel double threshold trust utilization scheme is proposed, which is shown to better than the conventional single threshold trust utilization approach.
- The performance of the proposed trust management system is investigated under various types of pollution attacks including bad-mouth attack, persistent attack, on–off attack, and collaborative attack. It is shown that the proposed trust management system is effective in defending against these attacks.

The rest of the paper is organized as follows. Section 2 gives an overview of the design of our trust management mechanism. Section 3 describes the proposed trust management system in detail. In Section 4, the performance of our trust management system under various types of pollution attacks is analyzed. In Section 5, several numerical examples are presented to validate the proposed studies. Finally, Section 7 concludes the paper.

2. System design overview

In this paper, we consider a mesh-based P2P streaming network [2–5], where all the peers can serve as the uploader and the downloader at the same time. In the proposed system, the media content is encoded and divided into small chunks by peers. Each peer maintains a buffer map announcing available and desirable chunks. Peers exchange their buffer maps, and then upload or download data chunks according to their interests. To defend against various potential attacks that are commonly seen in existing P2P streaming networks, we introduce a trust management system into the P2P streaming network. Under the proposed trust management system, each peer builds up trust records of other peers based on their previous direct transactions or recommendations from other peers. We refer to the trust built on direct interacting experience as direct trust, and refer to the trust built on recommendations from third party as indirect trust. A detail description of direct trust and indirect trust is given in Section 3.