Fighting Pollution Attack in Peer-to-Peer Streaming Networks: A Trust Management Approach

Xin Kang, Yongdong Wu

Fighting Pollution Attack in Peer-to-Peer Streaming Networks: A Trust Management Approach

Xin Kang and Yongdong Wu

Institute for Infocomm Research, 1 Fusionopolis Way, #21-01 Connexis, Singapore 138632
{xkang,wydong}@i2r.a-star.edu.sg

Abstract. Nowadays, peer-to-peer (P2P) streaming systems have become the most popular way to deliver multimedia content over the internet due to their low bandwidth requirement and high video streaming quality. 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 unique 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 in the design of the system. A new approach to model the direct trust is proposed, and a dynamic confidence factor that can dynamically adjust the weight of direct and indirect trust is also proposed. 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

The past decade has witnessed the rising of large-scale P2P multimedia streaming networks, over which millions of users interact with each other and exchange media contents in a distributed way. In these P2P streaming networks, peers are assumed to be well behaved and non-malicious. However, due to their distributed and dynamically changing infrastructure, P2P streaming 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.

As a matter of fact, a great deal of scholarly work has already published on the design of pollution-resistant mechanisms for P2P streaming systems. In [1], by measuring the PPLive streaming system, the authors showed that without any pollution-resistant mechanisms, the polluted content could spread through much of the P2P network. In [2], blacklisting and reputation mechanisms were proposed to avoid polluted content dissemination and isolate malicious peers. While in [3], the authors proposed a trust management system to defend strategic polluters who could upload polluted and clean chunks alternatively to avoid being detected. Trust management mechanisms for P2P applications have also been extensively studied in literatures [4–7]. However, trust is in nature a complex psychological concept involving a lot of complex properties,

the methodology used to model the trust has a significant influence on the performance of the trust management system. Trust models should be designed 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 kinds of pollution attacks for P2P streaming systems. The main contributions of this paper are as follows.

- A theoretic framework on the modeling of the trust management system for P2P streaming systems to fight against pollution attack 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 shown that the proposed trust model is effective in defending against the on-off pollution attack.

2 Trust Management in P2P Streaming Networks

In our trust management system, we use $T_{i,j}(t)$ to denote the trust that user i has on user j at time t. The value of $T_{i,j}$ is within the range $[0, 1]$, with "0" denoting distrust and "1" denoting fully trust.

Let $D_{i,j}(t)$ and $I_{i,j}(t)$ denote the direct trust and indirect trust that user i has on user j at time t, $T_{i,j}(t)$ can then be computed as follows

$$T_{i,j}(t) = \alpha_{i,j} D_{i,j}(t) + (1 - \alpha_{i,j}) I_{i,j}(t), \tag{1}$$

where $0 \leq \alpha_{i,j} \leq 1$ is a parameter reflecting user i's confidence of its direct trust over user j. A larger value of $\alpha_{i,j}$ indicates that user i is more confident of its own judgement of user j, while a smaller value of $\alpha_{i,j}$ indicates that user i relies more on other peers' recommendation on user j. For notation convenience, we drop t in the following discussion.

2.1 Confidence Factor

Different from the existing literatures (such as [3]) that use a constant to adjust the weight between the direct trust and the indirect trust, in this paper, we define a dynamic *confidence factor* $\alpha_{i,j}$, which is given as

$$\alpha_{i,j} = f\left(N_{i,j}^T\right), \tag{2}$$

where $f(\cdot)$ is a function, and $N_{i,j}^T$ denotes the number of direct transactions that has been made between user i and j at time t.

Basically, $f(\cdot)$ should have the following properties:

- $\forall N_{i,j}^T \in [0, +\infty)$, $f(N_{i,j}^T) \in [0, 1]$.

- $f(0) = 0$, and $\lim_{N_{i,j}^T \to \infty} f(N_{i,j}^T) = 1$.
- $f(N_{i,j}^T)$ is a monotonic increasing function of $N_{i,j}^T$.

Remark: (a). The first property guarantees that the value of the trust defined in Equation (1) falls within the range $[0, 1]$. (b). The second property captures the fact that when there is no direct transaction between user i and user j, user i can only rely on the indirect trust values gathered from other peers to determine its trust of user j. When the number of direct transactions between user i and user j is sufficiently large, user i can ignore the indirect trust. (c). The third property captures the fact that the confidence of user i on its own judgement of the trustworthy of user j increases when the number of direct transactions between them increases. (d). It is observed that these properties of $f(\cdot)$ are similar to those of cumulative distribution functions (CDF) of random variables. Therefore, the design of $f(\cdot)$ can borrow ideas from the probability theory.

In this paper, we propose two schemes that satisfy all the properties mentioned above to design the confidence factor $\alpha_{i,j}$. The two designs are given as follows.

$$\underline{\textit{Confidence Factor Design A (CFDA):}}\ \alpha_{i,j} = \frac{N_{i,j}^T}{N_{i,j}^T + c}, \tag{3}$$

where c is a positive constant.

$$\underline{\textit{Confidence Factor Design B (CFDB):}}\ \alpha_{i,j} = 1 - \beta^{N_{i,j}^T}, \tag{4}$$

where $0 < \beta < 1$ is a constant. It is worth pointing out that the value of c and β have a significant impact on the increasing rate of $\alpha_{i,j}$. In practice, they can be designed as a tunable parameter that can be tuned by users depending on the network environment.

2.2 Direct Trust

Direct trust is the trust of a peer on another peer based on their direct interacting experience. It is established only based on previous direct transactions between peers. Let $N_{i,j}^c(t)$ and $N_{i,j}^p(t)$ denote the total number of clean chunks and polluted chunks that user i has received from user j at time t, the direct trust $D_{i,j}(t)$ that user i has on user j at time t can be defined as

$$D_{i,j}(t) = e^{-\rho N_{i,j}^p(t)} \frac{N_{i,j}^c(t)}{N_{i,j}^c(t) + \eta}, \tag{5}$$

where ρ and η are positive constants, and $e^{(\cdot)}$ is the exponential function. It is easy to verify that the value of $D_{i,j}$ is within the range $[0, 1]$, and $D_{i,j}$ is an increasing function with regard to $N_{i,j}^c$ and a decreasing function with regard to $N_{i,j}^p$. It is worth pointing out that the proposed direct trust model is shown to be resistant to on-off attacks when ρ and η satisfy certain conditions.

Proposition 1: The trust management scheme $D_{i,j}(t) = e^{-\rho N_{i,j}^p(t)} \frac{N_{i,j}^c(t)}{N_{i,j}^c(t)+\eta}$ is resistant to on-off attack when $\rho > \ln(1 + \frac{1}{\eta})$.

Proof. The proof is omitted here due to the space limitation.

2.3 Indirect Trust

Indirect trust is the trust of a peer on another peer obtained via third-party peers' recommendations. Indirect trust is important when two peers have little or no direct interactions. Indirect trust is established through trust propagation, i.e., trustworthy peers are more likely to give honest feedbacks than distrusted peers. Indirect trust is determined by two key factors: the credibility of the third-party peer and its recommendation value of the trustee. In this paper, we define the indirect trust as

$$I_{i,j}(t) \triangleq \frac{\sum_{k \in S_{i,j}(t)} C_{i,k}(t) R_{k,j}(t)}{\sum_{k \in S_{i,j}(t)} C_{i,k}(t)}, \tag{6}$$

where $S_{i,j}(t)$ denotes the set of peers that has direct transactions with both peer i and peer j. $C_{i,k}(t)$ is the credibility of peer k, and $R_{k,j}(t)$ is user k's recommendation value of user j based on their interaction experience. In this paper, we let $C_{i,k}(t) = D_{i,k}(t)$ and $R_{k,j}(t) = D_{k,j}(t)$, where $D_{i,k}(t)$ is the peer i's direct trust on peer k, and $D_{k,j}(t)$ is the peer k's direct trust on peer j.

2.4 Trust Updates

Intuitively, recent interactions should have more weight than old interactions in computing the trust. Here, we assume that the interactions made within the recent Δt time have the same weight, and the weight of the interactions made older than Δt will experience certain attenuation. Mathematically, the update functions can be written as

$$N^c_{i,j}(t') = e^{-\lambda \Delta t} N^c_{i,j}(t) + \left(N^c_{i,j}(t') - N^c_{i,j}(t) \right), \tag{7}$$

$$N^p_{i,j}(t') = e^{-\mu \Delta t} N^p_{i,j}(t) + \left(N^p_{i,j}(t') - N^p_{i,j}(t) \right), \tag{8}$$

where λ and μ are positive constants, and $t' = t + \Delta t$. In this paper, we refer to λ and μ as *forgetting factor* and *forgiving factor*, respectively and request $\lambda > \mu$. This makes our trust management system remembers the unpleasant interactions longer than the pleasant interactions, which further increases our system's resistant to on-off attacks.

2.5 Utilization of Trust Values

With the trust management system introduced in this section, peers can easily compute the trust values of other peers. The trust values can then be used by peers to identify polluters, and to determine whether to perform a transaction with another peer. Suppose peer i decides to make a transaction with peer j with probability $p_{i,j}(t)$ at time t, then $p_{i,j}(t)$ can be determined by

$$p_{i,j}(t) = \begin{cases} 0, & \text{if } T_{i,j}(t) < \theta^P_i, \\ \chi_{i,j}, & \text{if } \theta^P_i \le T_{i,j}(t) < \theta^G_i, \\ 1, & \text{if } T_{i,j}(t) \ge \theta^G_i, \end{cases} \tag{9}$$

where $\chi_{i,j}$ is a constant, θ^P_i and θ^G_i are the thresholds for peer i to identify malicious and good peers, respectively. It is worth pointing out that peer i can set different $\chi_{i,j}$ for different peer j, depending on the content of the potential transaction. For example, peer i is willing to set a high value of $\chi_{i,j}$ for a peer j that has data chunks which are closer to its playback time.

3 Performance Evaluation under Potential Attacks

In this section, we give an introduction of the commonly seen attacks [1–3] in P2P streaming networks, such as *bad-mouthing attack* and *on-off attack*. The performance of the proposed trust management system are then investigated under these attacks.

3.1 Bad-Mouthing Attack

Bad-mouthing attack refers to the scenario that a single malicious peer or a group of malicious peers deliberately provides negative recommendations to frame up good peers.In our trust management system, the following two ways are adopted to fight against bad-mouthing attacks: (a). *Filtering out potential malicious recommendations*. When computing the indirect trust $I_{i,j}(t)$, peer i only select the top K peers based on the value of $D_{i,j}(t)$ from the set $S_{i,j}(t)$. Through this way, malicious recommendations from untrustworthy peers can be effectively avoided. (b). *Reducing the weight of indirect trust*. Bad-mouthing attacks are unavoidable as long as recommendations are taken into consideration. Therefore, reducing the weight of indirect trust in computing the trust is a good way to defend against bad-mouthing attacks.

The performance of our trust management system under the bad-mouthing attack is shown in Fig. 1. In this experiment, we let peer j keep uploading clean chunks to peer i. We assume that some malicious peers give bad recommendations on peer j for 80 percent of time. Peer i computes the trust values of peer j for 50 interactions based on the constant confidence factor scheme ($\alpha_{i,j} = 0.5$) and our dynamic confidence factor scheme, respectively. It is observed from Fig. 1 that the proposed dynamic confidence factors can effectively reduce the weight of indirect trust, and thus greatly increase our trust management system's resistant to the bad-mouthing attack.

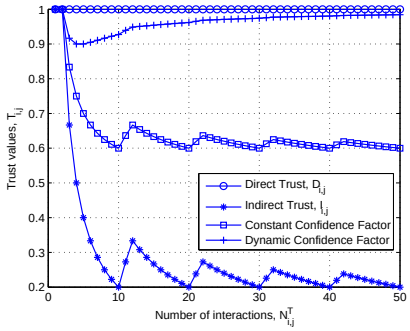

Fig. 1. Performance under bad-mouthing attacks

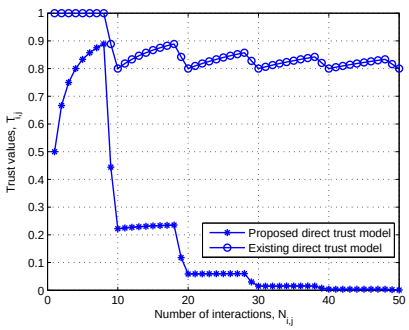

Fig. 2. Performance under on-off attacks

3.2 On-Off Attack

On-off attack refers to the scenario that a malicious peer sends clean and polluted chunks alternatively to other peers with an aim to keep its trust value above certain

threshold, and thus avoid being identified as a polluter. The on-off attack exploits the fact that most of the trust management mechanisms are designed to tolerate certain levels of unintentionally polluted chunks (such as incomplete and erroneous data chunks) due to bad network conditions. To combat the on-off attack, an effective way is to design a trust management system in which the dropping rate of trust value is larger than its increasing rate, i.e., the trust value drops sharply when the peer uploads polluted chunks, and accumulates slowly when the peer uploads the same number of clean chunks.

The performance of our trust management system under the bad-mouthing attack is shown in Fig. 2. In this experiment, peer j performs on-off attacks (20% on-off rate) to peer i. The trust values of peer j are computed for 50 interactions based on the existing direct trust model (EDTM) given in [7] and proposed direct trust model (PDTM), respectively. It is observed from Fig. 2 that the dropping rates are much larger than the increasing rate under PDTM. Therefore, the trust values obtained under PDTM are gradually decreasing in the long run. On the other hand, it is observed that the trust values computed under EDTM are maintained above certain thresholds, which indicates that EDTM is not resistant to the on-off attack.

4 Conclusion

In this paper, a trust management system to fight against various kinds of pollution attacks for P2P streaming systems are proposed by exploring the unique features of pollution attacks. 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 fighting against the bad-mouthing attack. Guidelines on how to deign such a dynamic confidence factor are given, and two specific designs of the dynamic confidence factor are proposed. Besides, a novel direct trust model that is proved to be resistant to the on-off pollution attack is proposed and investigated.

References

1. P. Dhungel, X. Hei, K. W. Ross, and N. Saxena, "The pollution attack in p2p live video streaming: measurement results and defenses," in *ACM SigComm Workshop on P2P streaming and IP-TV*, Kyoto, Japan, Aug. 2007.
2. A. Borges, J. Almeida, and S. Campos, "Fighting pollution in p2p live streaming systems," in *IEEE Int. Conf. on Multimedia and Expo*, Hannover, Germany, Jun. 2008.
3. B. Hu and H. V. Zhao, "Pollution-resistant peer-to-peer live streaming using trust management," in *IEEE Int. Conf. on Image Processing (ICIP)*, Cairo, Egypt, Nov. 2009.
4. S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The eigentrust algorithm for reputation managment in p2p networks," in *ACM WWW Conf.*, Budapest, Hungary, May. 2003.
5. L. Xiong and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowledge and Data Eng.*, vol. 16, no. 7, pp. 843–857, Jul. 2004.
6. R. Zhou and K. H. Wang, "Powertrust: A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Trans. Parallel and Distributed Systems*, vol. 18, no. 4, pp. 460–473, Apr. 2007.
7. Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modelling and evaluation for ad hoc networks," *IEEE J. Select. Areas Commun.*, vol. 24, no. 2, pp. 305–317, Feb. 2006.