Fighting Attacks In P2P Live Streaming. Simpler is Better.

Alex Borges Vieira, Advisors: Sergio Campos and Jussara Almeida
{borges, jussara, scampos}@dcc.ufmg.br
Computer Science Department - Federal University of Minas Gerais (UFMG)
Av. Antonio Carlos 6627 - ICEx - sala 4010 - Pampulha - Belo Horizonte - MG - Brazil - ZIP 31270-010

I. Introduction

P2P live streaming applications are becoming more popular each day. In contrast to the client-server model, the P2P approach overcomes problems such as system scalability and need for powerful resources in a single point. However, P2P networks may suffer from attacks and opportunistic behaviors. In this paper we present a decentralized reputation system to fight attacks in P2P live streaming networks which is simpler than previously proposed mechanisms. It allows peers rehabilitation and also permits interaction with potential polluters while they are acting fairly. In case polluters initiate an attack, peers can quickly identify and isolate them. Our results show that the overhead to block polluters is very small compared to the retransmission imposed by polluted data. During an attack, nodes in the proposed P2P system need a retransmission peak of 50% of the original media, while in previous systems they may need more than 100%. Moreover, the proposed system identifies and blocks pollution almost two times faster than other systems and under polluters collusion, it can handle situation without a significant overhead.

II. Fighting Attacks: Analysis and Discussion

Recently, it has been observed a growing interest of the academy and industry in P2P live streaming media applications. In this context, there are many studies to structure P2P networks for live streaming [1], [2]. These studies focus mainly on the maintenance of the service without interruption. However, users may have an opportunist or malicious behavior. Thus, some works have examined how selfish nodes can affect and interrupt the expected functioning of P2P streaming systems [3]–[5].

This work focuses on the detection of malicious peers and on counter-attacking these peers in a P2P live streaming system. In particular, we treat pollution attacks, where polluters tamper or forge streaming contents. Existing technics [6], [7] address pollution in P2P live streaming by simply checking media integrity. The source of the streaming marks the data (i.e. hash code) and each client checks its integrity. This approach can lead to a high retransmition rate, even if the number of polluters in the system is small [8].

To fight attacks in a P2P live streaming system, we propose a new reputation mechanism that does not rely in centralized authorities and is simpler than previously proposed systems [8], [9]. In our mechanism, each peer monitors actively all data exchanges with each partner to compute its reputation.

In the decentralized reputation model adopted by [8], [10], [11], a node p_i computes the reputation of a partner p_j based on two components: the individual experience and the network testimonial. In the new simplified approach, the node p_i takes into account only its individual experience with the node p_j.

A node p_i computes the individual experience with p_j similarly to the previous method [8]. More precisely, as shown in Equation 1, node p_i periodically computes p_j reputation based on the fraction of polluted chunks received from p_j. Let say that during a time period, p_i requests r chunks from p_j ($r > 0$), and that p_j's response includes n polluted chunks ($0 \leq n \leq r$). If $n/r \leq limit$ (limit is a value chosen by p_i), p_i considers its interaction with p_j as good, thus increasing its reputation score. Otherwise, p_i decreases p_j's local reputation.

$$R_i[p_j] = \begin{cases} max(0, R_i[p_j] - \alpha_{p_i} * (1 + n/r)^{y_i} & \text{If } n/r > NR_i \\ min(1, R_i[p_j] + \alpha_{g_i} * (1 + n/r) & \text{Otherwise} \end{cases} \quad (1)$$

If partner p_j's reputation becomes low ($R_i[p_j] < R\text{min}_i$, where $R\text{min}_i$ is a threshold value chosen by p_i), peer p_i stops its partnership with p_j. In order to allow peer rehabilitation, we proposed a new dynamic threshold mechanism. Lets define two P2P system states. The system may be under a calm, where polluters are not attacking, or the P2P system may be under a storm, where system is under a combined attack. If the P2P system is under calm, peers may change the threshold value to block attackers faster. Otherwise, peers may relax threshold value. To define if system is under a storm, peer p_i monitors several attempts to deliver polluted data. If p_i receives polluted data from more than one partner, it may think that system is under an attack and raises the value of the minimum acceptable reputation for its partners. If the opposite occurs, and p_i does not identify polluted data on consecutive interactions, p_i can interpret that the network is going through a calm and relax the minimum threshold.

$$R\text{min}_i = \begin{cases} min(Rt_{max_i}, R\text{min}_i + \gamma_{p_i}) & \text{Storm} \\ max(Rt_{min_i}, R\text{min}_i - \gamma_{g_i}) & \text{Calm} \end{cases} \quad (2)$$

Equation 2 shows the dynamic threshold mechanism. The minimum acceptable reputation ($R\text{min}_i$) may vary from Rt_{max_i} (worst storm state) to Rt_{min_i} (best calm state). We make $\gamma_{p_i} > \gamma_{g_i}$, so $R\text{min}_i$ increases faster.

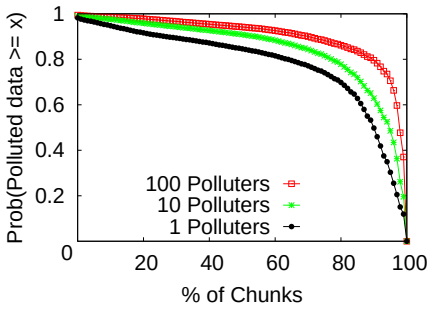

Fig. 1. Pollution Damage in the System.

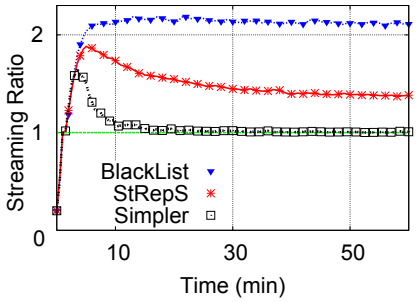

Fig. 2. Fighting Attacks Approaches Comparison.

III. Evaluation

Our results are mean values of 15 simulation executions (about 300,000 interaction per node), with a c.v. $< 1.4\%$.

We start discussing results for a system without reputation or data checking. Figure 1 shows situation for 1, 10 and 100 polluters in a mesh-based system with 1000 nodes (i.e. Sopcast). In a P2P system with just one polluter, about 80% of the nodes get at least 60% of polluted data.

Figure 2 shows a comparision of a centralized blacklist, the previously reputation-based system StRepS [8] and the our newer approach. In a system without attacks, peers may receive 1 data streaming ratio. If attack occurs, peers have to download more data due retransmission. We note that even if we perform a data integrity check and blacklist bad peers, they still cause considerable damage to the system. Peers must download more than 100% of extra data. The StRepS can detect malicious peers but, as attackers dissimulate their behavior, they remain in the system due to the network component of the reputation. While an attacker is polluting some nodes, it does not pollute some others and so, it may have a chance to interact again and cause more damage.

When nodes use the new method, they do not receive dissimulated testimonials from polluters. While an attacker is acting fairly, nodes may get its chunks. When an attacker starts to pollute, peers quickly take a local decision to avoid its bad data. The overhead after the initial attack is insignificant compared to StRepS, which needs about 30% more bandwidth.

Finally,Figure 3 shows a P2P streaming system under combined attacks and dissimulated patterns. In this figure, D represents the probability that all polluters do a combined attack in a small interval of time (burst time about 30 seconds). In all cases, the new reputation system is capable to detect an attack and avoid polluted data. Compared to Figure 2, the time to treat initial attack is almost the same in all cases.

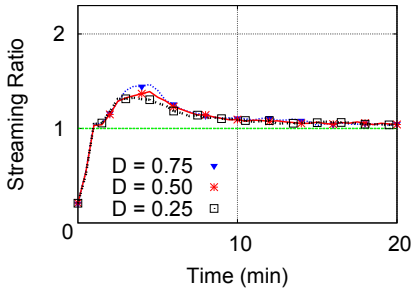

Fig. 3. Dissimulated Attackers.

IV. Summary

In this work we present a decentralized reputation system to fight attacks in P2P live streaming networks that is simpler and can also be much more effective than previously proposed mechanisms. It allows peers rehabilitation and also identifies dissimulated attackers.

Our new approach achieves its best performance almost two times faster than the traditional P2P reputation system. During an attack period, the simpler way needs a retransmission peak of 50% of the original media, while previous systems need a 100% more. Under polluter's collusion, our new simpler method can handle situation without a significant overhead, while others methods like blacklist need almost 100%.

Future work includes further evaluation of reputation systems, specially under combined attacks and heterogeneous network scenarios. Moreover, we intend to prototype as well as experiment with in a real P2P live streaming setup.

References

[1] Qi Huang, Hai Jin, and Xiaofei Liao, "P2p live streaming with tree-mesh based hybrid overlay", in *ICPPW '07: Proceedings of the 2007 International Conference on Parallel Processing Workshops*, Washington, DC, USA, 2007, p. 55, IEEE Computer Society.

[2] Chao Liang, Yang Guo, and Yong Liu, "Hierarchically clustered p2p streaming system", in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 2007, pp. 236–241.

[3] Xing Jin, S. Chan, Yongqiang Xiong, and Qian Zhng, "Detecting malicious hosts in the presence of lying hosts in peer-to-peer streaming", in *IEEE ICME, Toronto, Canada*, 2006.

[4] William Conner, Klara Nahrstedt, and I. Gupta, "Preventing dos attacks in peer-to-peer media streaming systems", in *13th Annual Multimedia Computing and Networking Conference,MMCN'2006*, San Jose, CA.

[5] Y Tang, L Sun, M Zhang, S Yang, and Y Zhong, "A novel distributed and practical incentive mechanism for peer to peer live video streaming", in *IEEE ICME, Toronto, Canada*, Jul 2006.

[6] P. Dhungel, X. Hei, K.Ross, and Saxena, "The pollution attack in p2p live video streaming: Measurement results and defenses", in *Proc. SIGCOMM Peer-to-Peer Streaming and IP-TV Workshop*, 2007.

[7] Maya Haridasan and Robbert van Renesse, "Securestream: An intrusion-tolerant protocol for live-streaming dissemination.", in *Journal of Computer Communications. Special issue on Foundation of Peer-to-Peer Computing.* Elsevier, 2007.

[8] Alex Borges, Jussara Almeida, and Sergio Campos, "Fighting pollution in p2p live streaming systems", in *IEEE International Conference on Multimedia & Expo,Hanover, Germany*, 2008.

[9] Alex Borges, Jussara Almeida, and Sergio Campos, "In portuguese: Fighting pollution in p2p live streaming", in *SBRC Brazilian Symposium on Computer Networks*, Rio de Janeiro, Brasil, 2008, SBC.

[10] Cristiano Costa, Vanessa Soares, Jussara Almeida, and Virgilio Almeida, "Fighting pollution dissemination in peer-to-peer networks", in *Proc. of the 2007 ACM symposium on Applied computing*, Seoul, Korea, 2007.

[11] Cristiano Costa and Jussara Almeida, "Reputation systems for fighting pollution in peer-to-peer file sharing systems", in *Proc. of the Seventh IEEE International Conference on Peer-to-Peer Computing, P2P'07.*