This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

ATTACK-RESISTANT COLLABORATION IN WIRELESS VIDEO STREAMING SOCIAL NETWORKS

W. Sabrina Lin, H. Vicky Zhao*† *and K. J. Ray Liu**

* ECE Dept., University of Maryland, College Park, MD 20742 USA
† ECE Dept., University of Alberta, Edmonton, AB T6G 2V4 Canada

ABSTRACT

Users using the same video streaming service within a wireless network share the same limited backbone bandwidth to the Internet. These users are motivated to collaborate with each other to obtain better-quality service. The decisions and actions of users influence the performance of others, hence they form a social network. In a fully-distributed wireless network, malicious attack can cause much more damage than over the Internet since the unstable wireless channel allows hostile users to mimic as a non-malicious user. Therefore, a robust attack-resistant cooperation strategy for non-malicious user is needed to combat the challenges in wireless networks. In this paper, we incorporate trust modelling into the cooperation among users to increase attack-resistance. Simulation results show our robust cooperation strategies can against 40% more attackers.

1. INTRODUCTION

With the explosive growth of network, multimedia signal processing, and communication technologies, millions of users share multimedia data over the Internet, and we witness the emergence of large-scale multimedia social networks. In such large scale social networks, users influence each other's decisions and performance. Although human-to-human dynamics is an area with growing importance, human factor seldom appears in signal processing analysis. Hence it raises a critical issue to formulate the complex user dynamics and analyze the impact of human factors on multimedia systems. Such investigation provides fundamental guidelines to the design of secure and personalized multimedia and networking services.

Peer-to-Peer (P2P) streaming network is one of the largest multimedia social networks on the internet, consisting of self-organized and distributed systems, with no centralized authority or infrastructure. Users in a P2P video-streaming social network watch video programs over networks simultaneously, and the system relies on voluntary contributions of resource from individual users to achieve high scalability and robustness and provide satisfactory performance. In past decades, the developments on wireless local area network enable users to utilize wireless connections [1] for various purposes, including joining the video-streaming network.

There are new challenges for streaming-user cooperation in a wireless network due to the weaker link. For example, the bandwidth of wireless channel is usually more limited than wired networks. Therefore, the users tend to be more greedy on utilizing the bandwidth when sharing with others. Furthermore, many of the users in the wireless networks have high mobility. Therefore, they would change physical positions from time to time and the quality of network connection may be unstable. Nevertheless, the unstable connection allows malicious users to act as non-malicious due to channel nature. All these factors motivate user seeking robust and attack-resistant cooperation strategies in wireless video-streaming social networks. To provide a better cooperation environment, we adopt Game theory [2] to model the interaction among users and to analyze the optimal cooperation strategies.

In the literature, a rank-based peer-selection mechanism was introduced in [3], where each user is ranked by a score. A peer with a higher score has more flexibility in peer selection, and thus receives better-quality videos.The work in [4] proposed a distributed incentive mechanisms on mesh-pull P2P video streaming systems, using layer video coding with a tit-for-tat strategy. However, the robust cooperation strategies for wireless P2P video streaming has not been discussed.

In this paper, we will focus on designing robust and attack-resistant cooperation strategies for wireless P2P video streaming social networks. We first study possible types of attack in the wireless video-streaming social network and introduce statistical detectors for malicious users. Then we will introduce the concept of trust and propose over-request method to fully utilize the cooperation channel.

The rest of this paper is organized as follows. Section 2 introduces the P2P wireless video-streaming system and the possible types of hostile attack. Section 3 introduces trust modelling and the optimal attack strategies. In Section 4 we show simulation results to evaluate the performance of the proposed strategies. Finally, Section 5 concludes this paper.

2. SYSTEM MODEL

In this section, we first describe the model of wireless video streaming systems and how two users in a wireless video streaming social network cooperate with each other. We then discuss the possible hostile behavior of the inside attackers, that is, the attackers also have legitimate identities, and their goal is to prevent selfish users from getting chunks.

2.1. Wireless Video Streaming Model

Here we assume that the wireless network service is provided by an access point connected to the Internet. The video bit stream is divided into media chunks of M' bits (equivalent to a t-second piece) at the server, and are channel-coded to M bits by the access point. The whole video, up to the playback time, is available at the streaming server on the Internet. Let there be a dedicated channel of bandwidth BHz for user cooperation and such a channel is different from the one connecting the access point and the users.

We focus on the scenario that video streaming will keep alive for a relatively long time, and there exist a finite number of users (for example, people watch live Super Bowl over the Internet). Each user will stay in the social network for a reasonably long time (for

The authors can be reached at wylin@umd.edu, vzhao@ece.ualberta.ca, and kjrliu@umd.edu.

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

instance, from the beginning to the end of the game). They are allowed to leave and reconnect to the network when necessary. Each user has an unique user ID registered at the first time he/she joins this network for identification purpose, and he/she uses the same ID whenever he/she reconnects to the same network. We consider an information-pull model, where the streaming server has no duty to guarantee the successful delivery of chunks and it only sends out chunks upon users' demand. For each user, uploading chunks to other users will incur cost, and successfully receiving chunks can improve the quality of his/her video and thus brings some gain.

The cooperation is done in a round-by-round manner. At the beginning of each round, the video-stream users exchange the information about the availability of each chunk in each user's buffer, and also declare the transmission power P_{min} used to transmit the chunks. Our previous work has shown that the users not only have no incentive to use transmit power different from what other users are using [6] but also are willing to use the same power as declared. After exchanging the buffer information, each user sends requests to other users, and at the same time keeps downloading from the original server. Each user is allowed to send multiple requests in each round, and he/she can also answer multiple requests. Let τ be the duration of each round. Then, the users either reply with the requested chunks and starts transmission or reject the request. After a round duration τ, the same request-answering process is repeated.

2.2. Malicious Attack

Handwash Attack: Since peer-to-peer system has an anonymous nature that each user is identified by the ID they registered, if a malicious user is detected and cannot cause damage to the system anymore, he/she can disable his/her ID and register for a new one to come back to the social network. By combining handwash with other types of attack, the malicious users can keep causing damage to the system as a new comer.

Incomplete chunk attack: A hostile user agrees to send the entire requested chunk to the peer, but sends only portions of it or no data at all. By doing so, the requesting user wastes his/her request quota in this round, and has to request the same chunk again in the next round. In general, not all cooperation decisions can be perfectly executed. For example, when a user decides to send another peer the requested chunks, packets of the chunk may not be correctly decoded at the receiver's side. In this paper, we assume that the requesting peer gives up the chunk if it does not arrive in one round, and we use P_{ij} to denote the probability of successful transmission of a chunk from peer i to peer j in one round of τ second.

Let $Cs^{(i)}(j,t)$ be the number of chunks user j agrees to send user i up to time t, and $Cu^{(j)}(i,t)$ be the number of chunks that user i successfully received from user j, To distinguish between transmission failure due to channel condition and intentional sending incomplete chunk, given a detection threshold $h > 0$, every selfish peer i can identify peer j as a malicious user by thresholding $Cs^{(i)}(j,t) - Cu^{(j)}(i,t)P_{ji}$ as follows:

$$\begin{aligned} j \in N_m^{(i)}(t) \text{ iff } & Cs^{(i)}(j,t) - Cu^{(j)}(i,t)P_{ij} \\ & \leq -h\sqrt{Cu^{(j)}(i,t)P_{ij}(1-P_{ij})}. \end{aligned} \quad (1)$$

In (1), $N_m^{(i)}(t)$ is the set of peers that are marked as malicious by peer i at time t, and $N_s^{(i)}(t)$ is the set of peers that are marked as selfish by peer i at time t.

Pollution attack: Pollution attack is a special hostile behavior in peer-to-peer systems [7]. In P2P wireless streaming systems, a malicious user replaces the data chunks with other video chunks and then releases this polluted content available for sharing with other peers. Unable to distinguish polluted chunks from unpolluted files, unsuspecting users download the polluted chunks into their own buffers. Since the polluted chunk is decodable, the users will not be able to know the chunk is polluted until its playback time. Therefore, between the time the chunk is received and it is played, it will stay in the users' butter and from which others may then download the polluted data. In this manner, polluted data chunks spread through the system.

Let $Cc^{(i)}(j,t)$ be the number of "unpolluted" chunks user i received from user j up to time t. Since non-malicious users might be unintentionally forward polluted chunks to other users, to control the damage caused by pollution attack, we adapt the credit-line mechanism as in our prior work [5] that

$$\begin{aligned} D^{(i)}(j,t) \leq D_{max}^{(i)}(j,t), \quad \forall t \geq 0, \text{where} \\ D^{(i)}(j,t) = Cc^{(i)}(j,t) - Cc^{(j)}(i,t). \end{aligned} \quad (2)$$

Here, $D_{max}^{(i)}(j,t)$ is the "credit line" that user i sets for user j at time t. The credit line is set for two purposes: 1) to prevent egoism when favors cannot be simultaneously granted and to stimulate cooperation between i and j, and 2) to limit the possible damages that j can cause to i. By letting $D_{max}^{(i)}(j,t) \geq 0$, i agrees to send some extra, but at most $D_{max}^{(i)}(j,t)$ chunks to j without getting instant payback. Meanwhile, unlike acting fully cooperatively, the extra number of chunks that i forwards to j is bounded to limit the possible damages when j plays non-cooperatively or maliciously.

3. ROBUST COOPERATION AND MALICIOUS USER DETECTION IN WIRELESS NETWORKS

In this section, we will first introduce the trust concept into the hostile user detection to improve attack-resistance. Later on, the optimal attack strategy will be discussed in order to show the worst-case scenario of the system under attack.

3.1. Trust Modelling

With handwash, malicious users can pretend to be innocent until being detected again. Hence non-malicious users suffer badly from the continuous damage caused by the malicious users and the unknown risk of interacting with untrustworthy users will reduce the incentive for cooperation in P2P wireless video streaming social networks. It takes several rounds of interaction to collect enough statistics using the malicious-user detector described in the previous section. Such a statistics collecting process allowing the handwashed malicious user to cause extra damage to the system. Thus to reduce the influence of handwash attack, non-malicious users have to identify malicious users as soon as possible.

Therefore, we introduce the idea of *trust* among selfish users. If a non-malicious user chooses several trusted users to share the interaction history with, the malicious user detection can be faster thus reduce the damage caused by handwash attack. Also, by taking the damage of the intrusted user j caused to other trusted users into credit line $D_{max}^{(i)}(j,t)$ can also stop cooperation with malicious users earlier.

Since the total number of users in a wireless video streaming social network will not be too large due to the coverage limit of the access point, direct trust model is sufficient for the users [8]. A selfish user i establishes direct trust with another user j upon observations on whether the previous interactions between user i and j are successful. We adopt the beta-function-based method in [9], where user

i trusts in user j at time t with value $Tr^{(i)}(j,t)$, which is defined as

$$Tr^{(i)}(j,t) = \frac{Cs^{(i)}(j,t) - C_p^{(i)}(j,t) + 1}{Cr^{(i)}(j,t) + 2}. \quad (3)$$

If user j is not malicious and also not serious polluted, based on the definition, $Tr^{(i)}(j,t)$ should be closed to P_{ij}. If user j mounts pollution attack, $C_p^{(i)}(j,t)$ will increase and if he/she mounts incomplete-chunk attack, $Cs^{(i)}(j,t)$ will decrease. Thus both types of attack decrease the numerator in (3), resulting in low trust value for malicious users. Also, the trust is directional, which means user i trusts user j does not imply that user j also trusts user i.

Since the trusted selfish users would like to identify the malicious users together, the damage caused by intrusted users to the trusted users are considered collectively. For example, if user i trusts another user j at round t, user i consider the damage that malicious user k has caused to user j as his/her own damage. This scenario is equivalent to reduce the credit line $D^{(i)}(k,t)$ in (2) to $D^{(i)}(k,t) - Tr^{(i)}(j,t) \times D^{(j)}(k,t)$. There is an effective bad-mouthing attack against the trust system, where malicious users provide dishonest recommendations to frame up good parties and/or boost trust values of malicious users. To resist such bad-mouthing attack, selfish users should only trust users who have sent them certain number of unpolluted chunks. Assume that selfish user i will only trust user j at time t if user j has sent i more than $Ch^{(i)}(t)$ useful chunks, that is, if $Cs^{(i)}(j,t) > Ch^{(i)}(t)$. The idea for setting $Ch^{(i)}(t)$ is that even the malicious user badmouthes on other selfish users, he/she has to be cooperative and pay enough cost to be trusted, by which the malicious user causes no damage, even contributes, to the system to be trusted. Another advantage of a peer-to-peer cooperation in wireless network is, everyone can listen to the chunk requests and chunk answering of all the users in the network, so the malicious user cannot arbitrarily badmouth the users that he/she has no interaction with.

In summary, the credit line $D_{max}^{(i)}(j,t)$ in (2) is updated in each round as follows:

$$\begin{aligned} & D_{max}^{(i)}(j,t+1) \\ & = \max\left\{1, D_{max}^{(i)}(j,t) - \sum_{k \in N_{Tr}^{(i)}(t)} Tr^{(i)}(k,t) \times D^{(k)}(j,t)\right\} \\ & \text{where } N_{Tr}^{(i)}(t) = \left\{k | k \in N_s^{(i)}(t) \text{ and } Cs^{(i)}(k,t) > Ch^{(i)}(t)\right\} \end{aligned} \quad (4)$$

And the malicious user detection is done at each round by

$$\begin{aligned} j \in N_m^{(i)}(t) \ \ \text{iff } & Cs'^{(i)}(j,t) - Cu'^{(j)}(i,t)p_{ji} \\ & \leq -h\sqrt{Cu'^{(j)}(i,t)p_{ji}(1-p_{ji})}, \\ Cs'^{(i)}(j,t) &= \sum_{k \in N_{Tr}^{(i)}(t)} Cs^{(k)}(j,t), \\ Cu'^{(i)}(j,t) &= \sum_{k \in N_{Tr}^{(i)}(t)} Cu^{(k)}(j,t), \\ \text{and } p_{ji} &= \frac{1}{\text{size of } N_{Tr}^{(i)}(t)} \sum_{k \in N_{Tr}^{(i)}(t)} \overline{P_{jk}}, \end{aligned} \quad (5)$$

if $Cu'^{(i)}(j,t)$ is large enough.

As will be demonstrated in Section 4, employing the trust model in (3) and replacing the modified credit line as in (4) will help improve the system's robustness against the handwash attack by malicious users and significantly increase selfish users' utility.

Based on the above discussion, we can conclude the **Multiuser attack-resistant cooperation strategy**: *In the peer-to-peer wireless video streaming, for any non-malicious user i, he/she initially marks every other user $j \neq i$ as non-malicious. Then, in each round t, i uses the following strategy:*

- *Update the credit line $D_{max}^{(i)}(j,t)$ by (4) and identify malicious users by (5)*
- *If i has been requested by j to send chunks, i will accept this request if j has not been marked as malicious by i and (2) holds; otherwise, i will reject the request.*
- *When i is requesting a chunk, he/she will send the request to peer j who satisfies $j = \arg\max_{j \in N_s^{(i)}(t), j \neq i} P'_{ji}$, where $P'_{ji} = P_{ji} \times Cc^{(i)}(j,t)/Cs^{(i)}(j,t)$ is the probability that user i successfully receives an unpolluted chunk from user j*

3.2. Optimal attack strategy

As discussed in [5], the damage that each attacker by pollution attack and incomplete-chunk attack can cause to selfish user i is bounded by $D_{max}^{(i)}$, which is negligible if the P2P wireless network has infinite lifetime. In this scenario, peer i will still waste his/her resource on the hand-washed malicious user j since i does not recognize j's new identity and every user is marked as non-malicious at the beginning. Therefore, with the hand-wash attack, malicious users can increase their payoff dramatically.

Theorem 1 In a wireless video streaming social network which every non-malicious user follows the cooperation strategy proposed in the previous section, if a malicious user i is not detected by any other users and if $D^{(j)}(i,t) < D_{max}^{(j)}(i,t)$ for all other users $j \in N$, hand wash will not provide the malicious user i any further gain. If the malicious user i is detected by another user j, or if there exists another user j where $D^{(j)}(i,t) \geq D_{max}^{(j)}(i,t)$, then the hand-wash attack will increase the malicious attacker i's payoff.

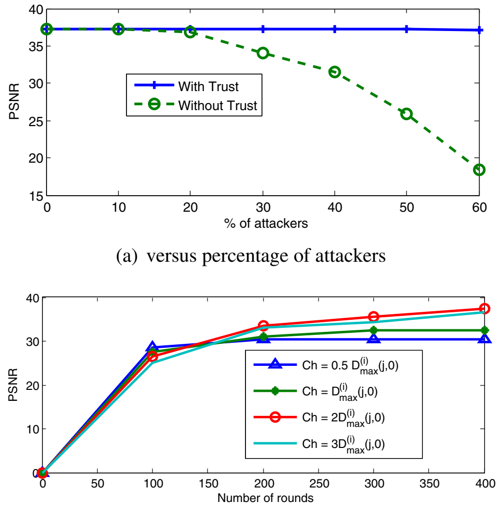
Proof. If the malicious user i is not detected by any other user and (2) is satisfied for all $j \in N$, then all the selfish users will still cooperate with the malicious user i. Using the original identity, i receives the same utility as he/she mounts the hand-wash attack and therefore, hand-wash will not bring the malicious user any extra gain. In the scenario where i is detected by a selfish user j as malicious and j refuses to cooperate with i any longer, if i chooses to hand-wash and reenters the game with a new ID, then j will cooperate with i until (2) is not satisfied or i is detected again. Therefore, in this case, i's payoff is increased by causing extra damage to the selfish user j.

From Theorem 1 and [5], *the optimal attacking strategy for a malicious user* is: Upon receiving a request an attacker $j \in Nm$ should always reject the requests; the attackers should always send requests to selfish users, until they do not agree to help, and hand-wash once he/she is identified malicious by one user in the social network. For a malicious use i, to determine whether it has been detected, he/she observes other users' behavior: a selfish user j will always reject the malicious user i's request if and only if i has been identified as malicious by j.

4. SIMULATION RESULTS

In our simulations, we assume the users communicate with the access point using IEEE 802.11 within the diameter of 20 meters, and users build their own wireless network that uses a different band dedicated to cooperation. The link from the wireless router to the Internet is a DSL link with 1.5Mbits download bandwidth. There are

978-1-4244-5637-6/10/$26.00 ©2010 IEEE



(a) versus percentage of attackers

(b) convergence speed respect to different trust threshold

Fig. 1. PSNR of the non-malicious users

totally 30 users in the network using video-streaming service, and another 5 users using Internet resources at the same time. For the 5 Internet users, we assume the traffic generated from them is a Poission process. The 30 streaming users will cooperate by sharing one channel, and we assume every one in the network can connect with any other user in the network via the dedicated cooperation channel. The location of users are randomly distributed within the circle of 20-meter diameter.

Figure 1 shows the averaged PSNR of the non-malicious users under different parameter setting. Here the attackers will mount hand-wash attack and the selfish users apply the cooperation strategy in Section 3. Figure 1(a) shows the robustness of the cooperation strategies with and without trust modelling versus the percentage of attackers. It is clear that trust modelling can significantly improve the attack resistance up to 60%. Figure 1(b) shows the non-malicious users' average PSNR under different trust thresholds Ch in (4) versus the number of rounds. It is clear after 400 rounds that the selfish user's PSNR is saturated and $Ch = 0.5D^{(i)}_{max}(j,0)$ or $Ch = D^{(i)}_{max}(j,0)$ gives lower PSNR than $Ch = 2D^{(i)}_{max}(j,0)$. These results imply that setting trust threshold Ch too small will cause damage to the system since the selfish users might trust the malicious users also. On the other hand, from Figure 1(b), higher Ch needs more number of rounds to saturate the selfish user's PSNR, which means the selfish users need to wait more rounds to trust other users.

Furthermore, we compare our cooperation strategy with the payment-based incentive schemes [10] and the resource chain trust model for P2P security [11]. The credit line is set to 100, and the users over request the chunk by 3 times. We first compare the attack-resistance of the three algorithm as shown in Figure 2. It is clear that our cooperation strategy is attack-resistant when the percentage of attackers is less than 60%, and the resource chain trust model can resist up to 30% of attackers. The payment-based method is not resistant to the attack, while under no attack the payment-based method can achieve 35 dB but still lower than the proposed cooperation strategy since the payment-based method does not consider the issues of wireless channels.

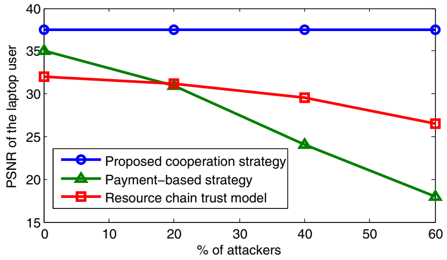


Fig. 2. Performance comparison of the proposed cooperation strategies, the payment-based cooperation strategy and the resource chain trust model

5. CONCLUSION

In this paper, we investigated the difficulties of cooperation in a wireless video streaming social network and improve the attack resistance to ensure system performance. We shown the optimal attack strategies and introduced the direct-trust concept into cooperation to against attack. Simulation results show that with trust modelling, the wireless video streaming system can against 40% more attackers, and the over-request algorithm also increase the PSNR of the users' video significantly.

6. REFERENCES

[1] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Key agreement in peer-to-peer wireless networks," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 467–478, Feb. 2006.

[2] G. Owen, *Game Theory*, Academic Press, 3rd edition, 2007.

[3] Ahsan Habib and John Chuang, "Incentive mechanism for peer-to-peer media streaming," *International Workshop on Quality of Service (IWQoS)*, pp. 171–180, June 2004.

[4] Zhengye Liu, Yanming Shen, Shivendra Panwar, Keith Ross, and Yao Wang, "Using layered video to provide incentives in p2p live streaming," *ACM Special Interest Group on Data Communication*, August 2007.

[5] W. Sabrina Lin, H. Vicky Zhao, and K. J. Ray Liu, "Incentive cooperation strategies for peer-to-peer live streaming social networks," *IEEE Transaction on Multimedia*, vol. 11, no. 3, pp. 396–412, April 2009.

[6] W. Sabrina Lin, H. Vicky Zhao, and K. J. Ray Liu, "Cheat-proof cooperation strategies for wireless live streaming social networks," *Proc. IEEE Int'l Conf. Acoustic, Speech, and Signal Processing (ICASSP)*, 2009.

[7] J. Liang, R Kumar, Y Xi, and K. Ross, "Pollution in P2P file sharing systems," *In Proceeding of IEEE Conference on Computer Communications (INFOCOM)*, vol. 2, December 2005.

[8] Y. Sun, Z. Han, and K.J. Ray Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Communication Magazine*, vol. 42, no. 6, pp. 112–119, Feb. 2008.

[9] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 42, no. 2, pp. 618–644, 2005.

[10] G. Tan and S. A. Jarvis, "A payment-based incentive and service differentiation mechanism for peer-to-peer streaming broadcast," *In Proceedings of International Workshop on Quality of Service (IWQoS)*, June 2006.

[11] Sinjae Lee, Shaojian Zhu, and Yanggon Kim, "P2P trust model: The resource chain model," 30 2007-Aug. 1 2007, vol. 2, pp. 357–362.