SIPTVMON: A Secure Multicast Overlay Network for Load-balancing and Stable IPTV Service Using SIP

Chia-Hui Wang, Yu-Hsien Chu and Tsa-Ta Wei
Department of Computer Science & Information Engineering
Ming Chuan University
Taoyuan County 333, Taiwan
{wangch@mail, s8366043@ss24, 99366512@ms1}.mcu.edu.tw

Abstract— **IPTV is an emerging multimedia network application over prevalent Internet. IPTV over P2P streaming network preserves significant advantages in scalability over conventional client-server architecture. IPTV media content delivered in P2P networks over public Internet still preserves the issues of privacy and intellectual property. In this paper, we use SIP protocol to construct a secure application-layer multicast overlay network, called SIPTVMON, with load-balancing and stability. SIPTVMON can secure all the IPTV media delivery paths against the eavesdroppers via elliptic-curve Diffie-Hellman (ECDH), SIP signaling and AES encryption. The proposed SIPTVMON also optimizes the load-balancing overlay tree by not only the link bandwidth to minimize the service latency, but also the life time to minimize the service degradations from frequent users' joins and leaving. The performance results from simulation and experiments in very large scale demonstrate the SIPTVMON's cost-effectiveness in quality of privacy protection and stability with good perceptual quality of objective PSNR values for IPTV.**

Keywords- IPTV; application-layer multicast overlay; privacy protection;load balancing; SIP; elliptic-curve Diffie-Hellman; AES.

I. INTRODUCTION

Due to the prevalent broadband Internet access and advanced video compression techniques, IPTV has been emerging as one of the most popular Internet applications. IPTV can further benefit Internet users by entertainment, social and business values, but IPTV faces more challenges of scalability, privacy and service quality over the public Internet due to conventional client-server architecture.

The success of well-known P2P video streaming systems such as PPStream, PPLive, Sopcast and TVants has proven that P2P paradigm is a feasible solution to deliver bandwidth-hunger IPTV media content in large scale over the pervasive Internet. However, the above-mentioned proprietary P2P video streaming systems still suffer the issues of long startup delays, significant video switching delays, large peer playback lags and security due to the peer heterogeneity and churn [1][2] [4].

Therefore, the P2P overlay networks for future multimedia networks (FMN) should overcome the previous shortcomings to further promise quality of service, security and experience to the IPTV end-users. Moreover, the FMN P2P overlay architecture for IPTV services should be not only easily convergent in heterogeneous networks, but also feasibly integrated with other Internet applications.

The logical topology applied in current P2P video streaming technologies is roughly classified into tree, mesh (i.e. multiple trees) and hybrid of tree and mesh [3]. Though tree-based P2P structure preserves simplicity, it is known vulnerable to peers' dynamics of heterogeneity and churn. Mesh-based P2P structure preserves more complex peer partnership, but it significantly improves the resilience to the dynamics from peers.

In this paper, we apply the well-known SIP signaling protocol [11] to construct a secure application-layer multicast (ALM) overlay network with load-balancing and stability for IPTV. The SIP-enabled secure multicast overlay network is called SIPTVMON and it's a tree-based overlay networks. To overcome the vulnerability of peers' heterogeneity and churn in tree-based overlay without significant overhead, we optimize the load-balancing SIPTVMON by the product of peers' link bandwidth and life time to achieve the stability.

The applied SIP protocol has been widely and successfully applied in many VoIP (Voice over IP) systems. The core of telecommunication's IP Multimedia Subsystem (IMS) [19] of 3G is also constructed by SIP signaling protocol. We believe that the proposed SIP-enable SIPTVMON not only can cooperate with SIP-based Internet applications like the prevalent VoIP applications, but also is feasible to help IMS in 3G mobile networks to achieve scalable IPTV service in cost-effectiveness.

The remainder of this paper is organized as follows. In Section II, we describe the related works of ALM overlay network, privacy protection and SIP signaling protocol. The details of proposed SIPTVMON are presented in Section III. Section IV describes simulation experiments for SIPTVMON and their performance results for P2P IPTV. Finally, we conclude the paper and future work.

The work was partially supported by National Science Council, Project No. NSC 99-2221-E-130-004, Taiwan.

II. RELATED WORK

We briefly review the related works in proposed solutions to construct an application-layer multicast overlay network with privacy protection, load-sharing and stability for scalable IPTV service.

A. Application Layer Multicast (ALM)

ALM is an application-level traversal method for IP multicast packets without the help from routers through unicast tunneling. ALM is also known as a cost-effective tool to construct overlay networks for large-scale Internet multimedia applications. ALM has the advantages of less overhead of maintenance than routers, provision of much larger multicast groups than IP multicast, less compatibility issues than IP multicast and easier extension to new features like security, error control, stability and etc.

Because routers usually disable the forwarding of IP multicast packets to prevent the flooding of multicast data, self-organization algorithms for effective transmissions in logical topology of multicast overlay network becomes the essential of ALM mechanism.

In our proposed SIPTVMON, a single-source ALM tree scheme is applied for its simplicity in not only the applied privacy protection, but also the tree adjustment in optimization of both scalability and stability for IPTV services.

B. Privacy protection for IPTV

For the cost-effective privacy protection of real-time video streaming in IPTV, Advanced Encryption Standard (AES) [10], which is a symmetric-key encryption standard adopted by the U.S. government, is most applicable to protect the voice data from eavesdropper over Internet. Since AES is a symmetric crypto system, thus it needs a key management infrastructure to issue a common secrete key (i.e. session key) for later video encryption/decryption between sender and receiver in IPTV.

As summarized in [13], three different methods of the session key distribution are pre-shared key, public-key encryption and the Diffie-Hellman (DH) key exchange [14]. The pre-shared key method has only a very small amount of data has to be exchanged. But, it will have the scalability issue in large group of talking peers. The public-key encryption can be used to create a scalable privacy-protection IPTV system and usually requires PKI (public key infrastructure) to distribute public key. Consuming much more resource than the pre-shared key is its disadvantage.

Generally, the third method of DH also has the scalability to protect large-scale IPTV services without the need of PKI. To prevent DH from the man-in-the-middle (MITM) attack, authentication [15] between sender and receiver are needed further. Thus, applying DH session key negotiation to protect IPTV services will consume more resource of bandwidth and computation than the previous ones but without the need of centralized PKI.

In SIPTVMON, we uses popular modified DH called elliptic curve DH (i.e., ECDH [17]) key exchange via SIP signaling protocol with much less computation overhead to construct the secure multicast overlay tree for IPTV's privacy protection.

C. SIP signaling for P2P IPTV

SIP [11] is the currently widely-used signaling standards for VoIP call setup and management (e.g., registration, resource administration, status, and capability exchange). Session Description Protocol (SDP)[12] is SIP's companion protocol to explicitly present parameters of functions applied in call set up and session management, such as the key exchange information for negotiating secret key for DH signaling. RTP (real-time transport protocol) [16] is the well-known application-layer protocol for deliver real-time media data like IPTV video packets.

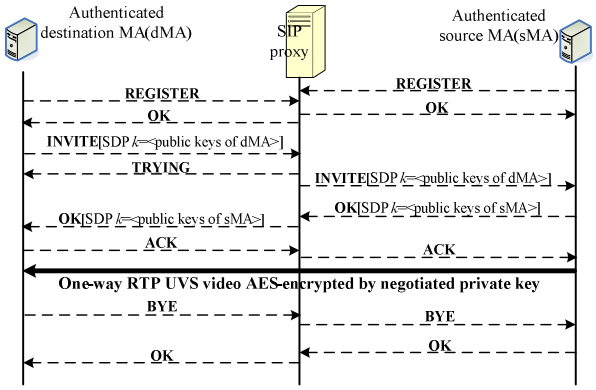

Figure 1. DH key negotiation via SIP/SDP signaling.

As shown in Figure 1, the option *k* in SDP within SIP can carry the public keys for DH signaling to negotiate a common secrete key for encrypting the IPTV video in RTP payload from source MA (sMA) to destination MA (dMA). Then, dMA can use this common secrete key to decrypt the encrypted RTP payload.

Since the SIP with companion SDP not only can handle the setup, modification, and tear-down of multimedia session, but also supports many extensions, enhancements, resource management and interworking with other heterogeneous systems, such as privacy protection mentioned above, transferring information during on-going session, instant messaging, and etc., SIP is the best signaling protocol over Internet for the control messages applied to furnished the proposed solutions of security, load-balancing and stability in SIPTVMON for scalable IPTV services.

III. SIPTVMON: SECURE ALM OVERLAY WITH LOAD-BALANCE AND STABILITY FOR IPTV USING SIP

SIPTVMON is an overlay network composed of a super agent SA (i.e. rendezvous) and different MAs on different multicast islands over Internet to effectively provide IPTV service for a dedicated media source from Content Server. A SIPTVMON's MAs are dedicated computer systems or software applications to receive a content data from sMA and then multicast it to their local subscribers, or unicast it again to one or more other dMAs over different multicast islands as illustrated in Figure 2. Besides, SA [9] will not only take the responsibilities to keep locations of MA and the detailed

topology information of SIPTVMON, but also help to forward the video from one source MA to the destination MA, which is located in a private multicast island, and etc. to furnish the ubiquitous IPTV service over the pervasive Internet.

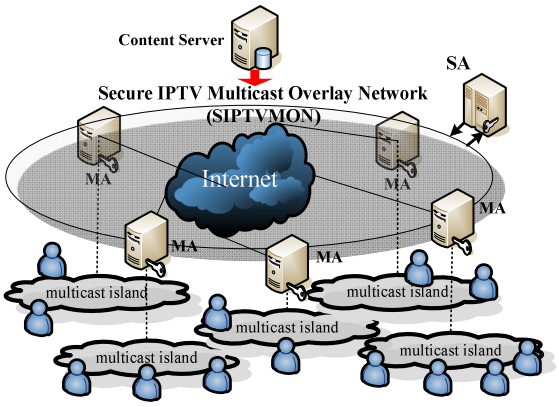

Figure 2. Primary SIPTVMON architecture.

However, the topology of SIPTVMON will change from time to time, because the Internet users can subscribe or unsubscribe the IPTV service at any time and then the corresponding MA may join or leave the SIPTVMON while either its local users subscribe or no user subscribes the IPTV service. Meanwhile, every dMA in its multicast island may preserve different capabilities of system resources and outbound network bandwidth to forward the media content, so we propose a load sharing scheme for SIPTVMON to prevent overloading sMA from jeopardizing perceptual quality of IPTV service for end users.

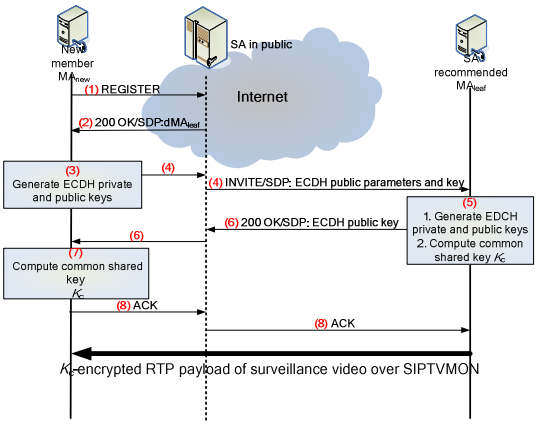

Figure 3. SIPTVMON's join procedures for a new MA (i.e. MA_{new}).

A. MA joins/leaves to/from SIPTVMON with security provision

According to the long tail theory of customer demographic [7], usually most of the customers like newly joined MAs of SIPTVMON won't stay with SIPTVMON for a long period. To further reduce the processing overhead of reconnecting disjoint trees in SIPTVMON while a non-leaf node of MA occasionally leaves from SIPTVMON, the new dMA should be joined to the leaf node of MA in SIPTVMON.

The procedures of a new MA joining to SIPTVMON are illustrated in Figure 3 and described as follows:

1. New MA denoted as MA_{new} sends a SIP "REGISTER" request with specified content identifier and registration identifier to SA to ask SA for the connection address of a leaf MA which the MA_{new} can be connected to join the SIPTVMON tree.
2. SA plays as roles of SIP proxy and oracle of SIPTVMON topology information to send back the SIP "OK" response with SDP body of corresponding connection address of a leaf node MA_{leaf}, which the new MA_{new} can be connected to SIPTVMON. Therefore, the SA must maintain all up-to-date SIPTVMON topology information to effectively and correctly reply the access request with a capable leaf node of handling the forwarding requested video to the new subscriber MA_{new}. That's the reason why SA is called the super agent.
3. After successful registration, MA_{new} needs to prepare the public parameters and key for the peer by ECDH key exchange algorithm. Elliptic curve [17] function's parameter $Eq_1(a_1,b_1)$,base point $G_1=(x_1,y_1)$ and a random private key k_{new} are generated by MA_{new}. Then, a public key P_{new} can be calculated by k_{new}, Eq_1 and G_1.
4. MA_{new} sends a SIP "INVITE" request message to remote MA_{leaf} via SA proxy. The SDP body in the SIP message includes the ECDH public data of Eq_1, G_1 and P_{new}.
5. While MA_{leaf} receives the MA_{new}'s "INVITE" message and MA_{new} is authorized to join the SIPTVMON, it will randomly generate a private key k_{leaf} and then calculate a public key P_{leaf} according to the k_{leaf} and received Eq_1 and G_1. Besides, the common private key K_c for encrypting video content can be computed by the k_{leaf}, received P_{new}, Eq_1 and G_1.
6. Then MA_{leaf} responses a SIP "OK" message with SDP body including the public key P_{leaf} back to MA_{new}.
7. While MA_{new} receives the public key P_{leaf} from MA_{leaf}'s SIP "OK" message, MA_{new} can use P_{leaf}, private key k_{new}, Eq_1 and G_1 to computer the common private key K_c to later decrypt the encrypted video.
8. Then, MA_{new} will send to MA_{leaf} a SIP "ACK" message via SA to confirm the completion of ECDH key exchange and member join to SIPTVMON. Meanwhile, SA can also update its SIPTVMON tree topology information of new member join accordingly.

While a non-leaf MA needs to leave from the SIPTVMON after its local users in multicast island sequentially unsubscribe the IPTV service and it has no obligation to forward video for other MAs (i.e. child nodes of the leaving MA), the child nodes must reconnect to other MAs in the SIPTVMON to continue the IPTV service.

As shown in the example of Figure 4, procedures of a non-leaf node MA_l leaving the SIPTVMON without breaking IPTV service of its child nodes are illustrated and the details are described as follows:

1. The MA_l will first send leaving requests of SIP "BYE" with SDP body of the video content identifier and its registration identifier to acknowledge not only its parent node to cease forwarding video later, but also its child nodes (i.e. MA_{c1} and MA_{c2}) to seek other new parent nodes of MA to replace their old parent MA_l for continuing IPTV video streaming.
2. The acknowledged child nodes (i.e. MA_{c1} and MA_{c2}) will send re-registration requests of SIP "REGISTER" with SDP body of the same video content identifier, their registration identifiers, and the reason of re-registration to the oracle SA to ask for the connection information of new parent nodes respectively.
3. SA will send back response messages of SIP "OK" with SDP body of the connection information of new parents (i.e. MA_{s1} and MA_{s2}) to the leaving-acknowledged child nodes (i.e. MA_{c1} and MA_{c2}).
4. The acknowledged child nodes for parent node's leaving will be able to directly send re-connect requests of SIP "INVITE" message with SDP body of the video content identifiers, their registration identifiers and the ECDH

public information like previous step *4* in new MA's join procedures to their new parent nodes (i.e. MA_{s1} and MA_{s2}) respectively.

5. The new IPTV connections will be immediately established from new parents to the leaving-acknowledged child nodes from the old parent, right after new parents (i.e. MA_{s1} and MA_{s2}) responds the positive SIP "OK" message via the oracle SA to acknowledged child nodes and leaving MA with SDP body of the corresponding video content identifier, corresponding registration identifier, and the ECDH public information like previous step *6* in new MA's join procedures respectively. Meanwhile, the sibling nodes MA_{s1} and MA_{s2} will start respectively forwarding video to children of MA_{c1} and MA_{c2}, and simultaneously the leaving MA_l stop forwarding video to to children of MA_{c1} and MA_{c2}.

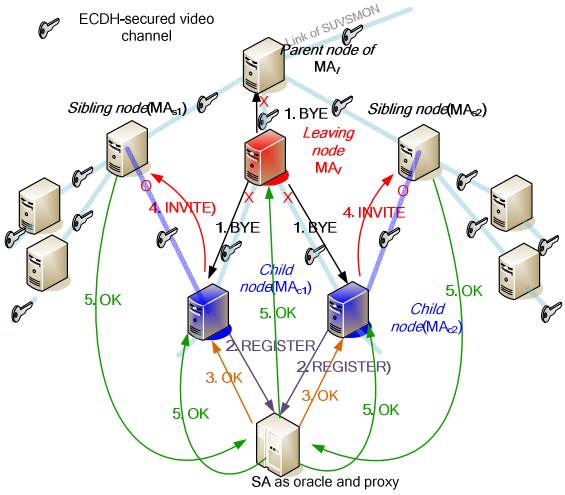

Figure 4. Message flow in leaving procedures of a non-leaf MA_l with two children.

Such gracefully leaving procedures for a non-leaf MA_l leaving from SIPTVMON can minimize the IPTV service disruption from subsequent video packets loss for the descendant nodes below the leaving node MA_l to maintain the overall quality of IPTV services for users.

Since all the SIP messages including request and response in the previous procedures in new MA's join and old MA's leaving will be forwarded via the so-called SIP proxy (i.e. oracle SA), these messages can easily help SA to update its details of SIPTVMON topology information to cost-effectively provide correct information upon later requests from SIPTVMON members.

B. Optimizations for SIPTVMON of load sharing and stability

As the SIPTVMON's member MAs, which preserve different capabilities of system resources and network bandwidth, may join, leave or fail in the overlay network of SIPTVMON during the IPTV service session, the avoidance of IPTV service disruption must be considered in proposed SIPTVMON architecture.

Because the larger outbound link bandwidth of MAs in SIPTVMON support not only higher bit rate of IPTV video, but also more connections to remote dMA with good quality of IPTV service, in previous researches [5][6], the ALM tree's node with more out-degree (i.e. higher bandwidth) should be moved to the top of the tree to perform the optimization of load sharing in overlay network to pursue better quality of service.

Furthermore, another important factor of optimization can affect stability of the SIPTVMON is the user lifetime, because Internet users may join and leave IPTV services in different timing. In the paper [18], authors presented that Internet user's lifetime in video streaming systems will follow the long-tailed distribution [7]. It means that just a few users will stay in the system for a long time and most of the users will stay in the system in a short time.

To apply both factors mentioned above, which may affect stability of overlay network, [6] uses the product of bandwidth and life time (i.e. Bandwidth and life-Time Product, BTP) for the load sharing optimization of overlay network. However, this BTP function is much sensitive to the variation of bandwidth on Internet to frequently reconstruct the overlay network. Therefore, we further propose improved criterion called ABTP (Averaging Bandwidth life-Time Product) to effectively minimize service disruption during optimization for SIPTVMON. The improved value function of ABTP is defined as follow:

$$ABTP = \frac{\sum_{i=1}^{n} Bandwidth_i}{n} \times lifetime \quad (1)$$

As shown in eq. (1), ABTP is evaluated as a criterion of load sharing optimization for SIPTVMON by averaging the latest *n* measured bandwidth values of a node (i.e. MA) and then multiplying by the value of this node's life-time in SIPTVMON. According to the ABTP value of each node in SIPTVMON, we can reconstruct the SIPTVMON such as the examples illustrated in Figure 5. At the left hand side of Figure 5, node M_2 preserved higher ABTP value than node M_1, node M_2 should be moved to higher level than node M_1. But, node M_1 preserved less degree than node M_2 and then node M_2 will link to the child nodes of parent M_1 for leaving them in the same level. Meanwhile, some of the child nodes of parent M_2 with larger ABTP values will be moved with parent M_2 to the upper layer to keep the degrees of nodes M_1 and M_2 unchanged. The example of optimized SIPTVMON tree is illustrated at the right hand side of Figure 5.

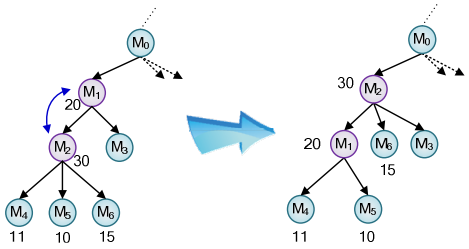

Figure 5. Example of ABTP optimization for a SIPTVMON tree.

Because the oracle SA also plays the role of SIP proxy, not only the running topology of SIPTVMON tree, but also both of MAs' bandwidth and life-time can be recorded by all the forwarded SIP messages in SA. Then, optimization score like ABTP can be calculated by SA and then SA can recommend the optimization procedures via the SIP "UPDATE" request messages to corresponding SIPTVMON's MAs participated in the on-going IPTV session to ask them to cooperate for the optimization. In SIP protocol, the request message "UPDATE" is designed to enable the modification of session information.

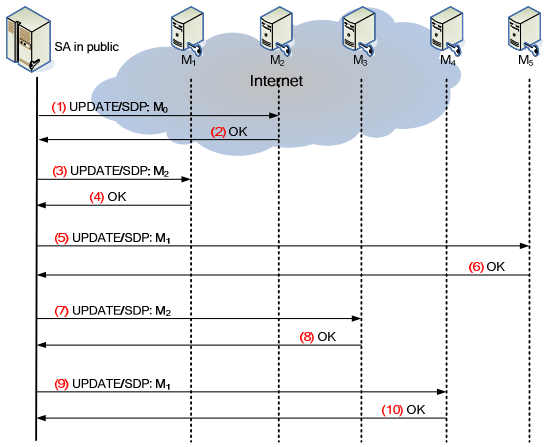

Figure 6. SIP message flow for SIPTVMON optimization in Figure 5.

As shown in Figure 6, the SIP messages flow is illustrated to accomplish the optimization of the example from Figure 5 and the procedures are described in details as follows:

1. Oracle SA detects the optimization score of M_2 at lower level is larger than the M_1 at higher level in SIPTVMON tree. SA sends M_2 the SIP "UPDATE" with the SDP body of M_2's video content identifier and registration identifier (for authentication) and the recommended new parent M_0's connection information.
2. After M_2 receives the recommendation of new parent from SA, it will first start the similar leaving procedures mentioned above but without acknowledging its children to re-join to other parents, and then M_2 with its children starts the join procedure with ECDH scheme mentioned above to connect to new parent M_0. While the join procedure is completed, M_2 sends the SIP "OK" response message to SA.
3. SA then sends M_1 with low optimization score the SIP "UPDATE" message with the SDP body of authentication identifiers and the recommended new parent M_2's connection information.
4. After M_1 receives the recommendation of new parent from SA, it will first start the similar leaving procedures mentioned above but without acknowledging its current children to re-join to other parents, and then M_1 with its current children starts the join procedure with ECDH scheme mentioned above to connect to new parent M_2. While the join procedure is completed, M_2 sends the SIP "OK" response message to SA.
5. Because M_1's child M_3 has been moved to lower level of SIPTVMON than M_2's children M_4, M_5 and M_6, M_3 with higher optimization score must first exchange position with M_2's child M_5 with the lowest score. Therefore, SA sends M_5 the SIP "UPDATE" message with similar SDP body to ask M_5 to reconnect to new parent M_1.
6. After M_5 rejoins to M_1 like previous steps, M_5 sends the SIP "OK" response message to SA.
7. Then M_1's child M_3 has to move to the same level as M_2's children. SA sends M_3 the SIP "UPDATE" message with similar SDP body to ask M_3 to reconnect to new parent M_2.
8. After M_3 rejoins to M_2 like previous steps, M_3 sends the SIP "OK" response message to SA.
9. Since the out degree of M_2 is higher than before, currently the child M_4 with lowest score must move to the lower level of M_2 with one available degree. Therefore, SA sends M_4 the SIP "UPDATE" message with similar SDP body to ask M_4 to reconnect to new parent M_1.
10. After M_4 rejoins to M_1 like previous steps, M_4 sends the SIP "OK" response message to SA to finish the procedures of optimization.

The adjustment of SIPTVMON tree for optimization of load-sharing and stability may incur the service disruption, but ABTP can smooth the variation of bandwidth on Internet to avoid unnecessary adjustment of SIPTVMON and then further effectively reduce the service disruption.

IV. Experiments and Performance of SIPTVMON

To demonstrate our proposed optimization scheme via *ABTP* criteria for SIPTVMON, we use the well-known simulation tool OMNeT++4.0 [8] to construct a vital SIPTVMON with new MAs joining, old MAs leaving and timely SIPTVMON adjustment for optimization at load-sharing and stability. The detailed simulation parameters and corresponding test values are listed in TABLE I.

TABLE I. Simulation Parameters for SIPTVMON.

Parameter	Values
MA quantity	*2000, 4000, 6000, 8000, 10000*
degree of MA	*2 to 5 out-degree (uniform distribution)*
link bandwidth	*Mean:400kbits, Std: 10, normal distribution*
link delay	*Mean:0.08s, Std: 0.05, normal distribution*
optimization (Opt.)	*Bandwidth only(B), Life time only(T), BTP, Averaging bandwidth only(ABO), ABTP*
simulation time	*20000 seconds*
Opt. cycle	*40 seconds*

During the simulation for SIPTVMON, we recorded the count of control messages and service disruptions, tree depths and service latency for different optimization criteria. We will perform each test case five times to find out the mean and standard deviation of these simulation results.

As shown in Figure 7, *ABTP* criterion outperforms less overhead of control message than the other four optimization criteria. Those criteria (i.e. *B* and *ABO*) without considering life time preserve more control message. It's because more possibility of high-level nodes leaving the SIPTVMON tree indicated more control messages are needed to repair the SIPTVMON for continuing IPTV service, if MA's life time is not considered in optimization for load sharing.

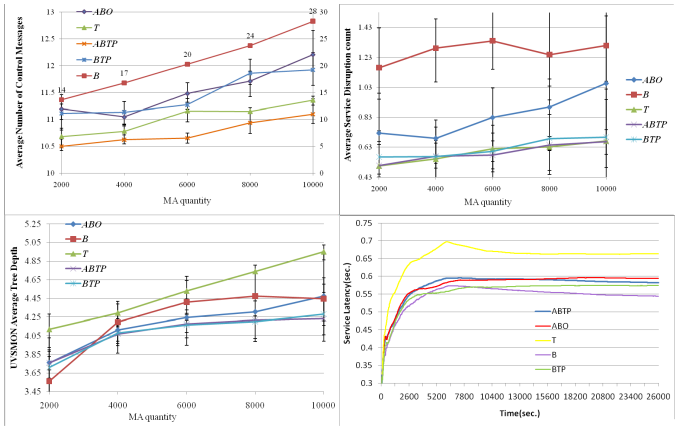

Figure 7. Average of control messages, service disruption, tree depths an service latency in different optimization criteria.

While an old MA leaving SIPTVMON or SIPTVMON's adjustment for load sharing, service disruption may occur to degrade the quality of IPTV video streaming service for those dMAs under detached parent in SIPTVMON. *ABTP* also

preserves less average count of service disruption to help SIPTVMON to achieve better quality of service. Besides, *ABTP* optimization criterion keeps lower depths of SIPTVMON tree than other criteria except test case of MA quantity 2000. Those optimization criteria without considering life time will keep less depth than others in most of test cases.

While the depth of SIPTVMON tree getting larger, the IPTV service latency of bottom dMA_s is also getting longer. For the test case of MA quantity 6000, the values of service latency will get more and more after simulation starts and the time goes by. It's because the tree is growing and the increasing depth indicates the increasing service latency. While the member of MA in SIPTVMON tree reaches 6000 and some of these MA may leave from the SIPTVMON tree, the service latency will stop increasing due to the adjustment of SIPTVMON tree through different optimization criteria. The optimization criterion *T* preserve much more service latency during simulation time than other criteria, since it didn't consider the bandwidth to effectively reduce both the depth of SIPTVMON tree and corresponding service latency.

ABO considers same criteria of bandwidth only with criterion *B*, but *ABO* preserve larger service latency than criterion *B*. This is because the averaging bandwidth from *ABO* won't decrease the tree depth of SIPTVMON in the same large scale as *B*. The reason why optimization criterion *ABTP* cannot achieve best results in service latency is because it considers both of the averaging bandwidth and life time. It's not very possible for criterion *ABTP* to outperform less service latency than criterion *B*.

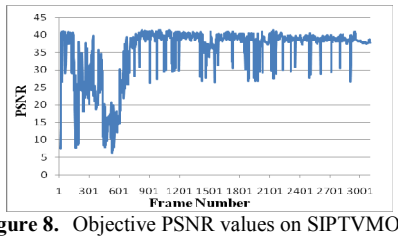

Figure 8. Objective PSNR values on SIPTVMON.

To validate the perceptual quality of IPTV video on SIPTVMON, we estimated the packet loss rates during the service disruption in above-mentioned simulations. Then, the estimated packet loss rates were applied to a recorded video of about 2-minute length to measure the objective PSNR values as shown in Figure 8. At the beginning of 10 to 20 seconds at the video, due to the optimization period was not started yet, the tested video preserves worse PSNR values than later periods after the optimization started.

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a secure overlay by application-layer multicast with load-sharing and stability schemes to cost-effectively provide scalable IPTV services. The proposed SIPTVMON can provide Internet users with scalable and stable IPTV video streaming with privacy protection, since the simulations and results demonstrate that our improved optimization via both averaging bandwidth and life time has not only the better performance in overhead of control message, service disruption, and tree depth than the other optimization criterion, but also preserve the good perceptual quality of objective PSNR values with privacy provision.

In the near future, we plan to deploy SIPTVMON over the global Internet test-bed (e.g. PlanetLab [20]). We will also investigate the reliability features of the packet cache and adaptive FEC to improve further the P2P IPTV's quality of service by SIPTVMON.

REFERENCES

[1] X. Hei, C. Liang, J. Liang, Y. Liu, K. W. Ross, "A Measurement Study of a Large-Scale P2P IPTV System," IEEE Transactions on Multimedia, pp.1672-1687, Vol.9, No.8, December 2007.

[2] X Hei, Y. Liu, K. W. Ross, "IPTV over P2P Streaming Networks: The Mesh Pull Approache," IEEE Communications Magazine, pp.86-92, February 2008.

[3] F Wang, Y. Xiong and J. Liu, "mTreebone A Collaborative Tree-Mesh Overlay Network for Multicast Video Streaming," IEEE Transactions on Parallel and Distributed Systems, pp.379-392, Vol.21, No.3 March 2010.

[4] D. Ciulo, et al., "Network Awareness of P2P Live Streaming Applications: A Measurement Study," IEEE Transactions on Multimedia, pp. 54-63, IEEE Transactions on Multimedia, Vol.12, No.1, January. 2010.

[5] S. E. Deering, "Multicast routing in internetworks and extended LANs," in Symposium proceedings on Communications architectures and protocols Stanford, California, United States: ACM, 1988.

[6] G. Tan and Jarvis S. A., "Improving the Fault Resilience of Overlay Multicast for Media Streaming," Parallel and Distributed Systems, IEEE Transactions on, vol. 18, pp. 721-734, 2007.

[7] Chris Anderson, "The long tail," in Wired, Oct. 2004.

[8] OMNet++, http://www.omnetpp.org/

[9] R.I. Chang, T.C. Wang, C.H. Wang, J.C. Liu, J.M. Ho, "Effective Distributed Service Architecture for Ubiquitous Video Surveillance," Journal of Information Systems Frontiers, 2010, http://www.springerlink.com/content/v688368mu017um6k/fulltext.html

[10] NIST, Advanced Encryption Standard, Federal Information Processing Standard 197, Nov. 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[11] J. Rosenberg, H. Schulzrinne, and et al., "Session Initiation Protocol (SIP)," IETF, RFC 3261, June 2002.

[12] M. Handley and V. Jacobson, "Session Description Protocol (SDP)," IETF, RFC4566, July 2006.

[13] J. Arkko, E. Carrara, F. Lindholm, M. Naslund and K.Norrman, "Multimedia Internet KEYing (MIKEY)," IETF, RFC 3830, August 2004.

[14] M. E. Hellman, "An Overview of Public Key Cryptography," IEEE Communications Magazine, pp.42–49, May 2002.

[15] C.C. Yang, R.C. Wang, W.T. Liu, "Secure Authentication Scheme for Session Initiation Protocol," ELSEVIER, Computer & Security, 24, P381-386, 2005.

[16] H. Schulzrinne and et al., "RTP: A Transport Protocol for Real-Time Applications," IETF RFC 3550, July 2003.

[17] D. Hankerson, A. Menezes, and S.A. Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag, 2004.

[18] K. Sripanidkulchai, A. Ganjam, B. Maggs, H. Chang, "The feasibility of supporting large-scale live streaming applications with dynamic application end-points," in Proceedings of the ACM SIGCOMM 2004, Portland, Oregon, USA.

[19] Gonzalo Camarillo, Migue A. Garcia-Martin, The 3G IP Multimedia Subsystem-Merging the Internet and the Cellular Worlds, John Wiley & Sons Ltd, 2004.

[20] PLANETLAB, an open platform for developing, deploying and accessing planetary-scale services, http://www.planet-lab.org/