ISSN : 2320-0790

COMPUSOFT
An International Journal of Advanced Computer Technology

A Secure Overlay Dynamic Multicast Network with Load Balancing for Scalable P2P Video Streaming Services

[1]Mr Prashant B Kumbharkar, [2]Dr.Trimbak Ramchandra Sontakke
[1]Research Scholar, [2]ResearchGuide
JJT University, Rajasthan (India)

Abstract: A creating mixed media Internet application P2p VIDEO-STREAMING over P2p system stops critical profit in adaptability. P2p VIDEO-STREAMING media substance conveyed in P2p organizes over open Internet still jam an issues of protection and licensed innovation rights. In this paper, we utilize SIP convention to build a safe application-layer multicast overlay system, called SALMON. SALMON can secure all media conveyance ways against meddlers by means of elliptic-curve Diffie-Hellman (EDH) key trade on SIP flagging and AES encryption. Its burden adjusting overlay tree is additionally advanced from associate heterogeneity and stir of companion joining and leaving to minimize both administration debasement and dormancy. An execution results show SALMON's expense viability in nature of protection ,stability from client churn, and great perceptual nature of destination PSNR values for versatile administrations over Internet.

Keywords:*SIP,SALMON,ALM,ABTP*

1. Introduction

P2P feature streaming confronts more difficulties of versatility, protection, and administration quality over an open Internet because of a routine customer server building design connected.

An achievement of generally called P2p feature streaming frameworks is demonstrated that P2p ideal model as an attainable answer for convey data transfer capacity hunger media content in substantial scale over a pervasive Internet. On the other hand, an aforementioned restrictive P2p feature streaming frameworks still endure an issues of long startup delays, huge feature exchanging deferrals, expansive companion playback slacks, and security because of an associate heterogeneity and stir [6–7]. Along these lines, a P2p overlay systems for future interactive media Internet ought to conquer a past deficiencies to further guarantee nature of service, security, and experience to end clients. Also, a P2p overlay structural planning for guaranteeing administrations ought to effectively concurrent in heterogeneous systems, as well as practically incorporated with other Internet applications.

In this paper, we apply SIP convention [8] to build an application-layer multicast (ALM) overlay system, which is called SALMON, with protection insurance, burden adjusting, and solidness to overcome hindrances in P2p feature streaming frameworks. Commitments in proposed SALMON are as takes after.

(i) Security Provision. The majority of a P2p feature streaming substance jelly licensed innovation rights, so a substance conveyance ways in SALMON tree are secured against Internet spies by means of elliptic-bend Diffie-Hellman (EDH) key trade calculation and AES encryption.

(ii)stability for Peer Heterogeneity and Churn. Since peers (i.e., clients) with regularly changing Internet access data transfer capacity may join and leave a P2p feature streaming administration whenever as they wish, we keep on optimizing SALMON overlay tree with least SIP flagging overhead to accomplish stable P2p feature streaming administration by a result of normal connection data transfer capacity and administration life time in companions.

(iii) Interoperability with Other Internet Applications. A connected SIP convention has been generally and effectively conveyed in Voice over IP (Voip) applications. Also, a center of IP Multimedia Subsystem (IMS) in 3g telecom is likewise developed by SIP convention.

We accept that a proposed SALMON schema not just can collaborate with SIP-empowered Internet applications like pervasive Voip applications, additionally is doable to help IMS in 3g versatile systems to attain adaptable P2p feature streaming administration procurement in more practical way.

A rest of this paper is composed as takes after. In Section 2, we depict a related works of ALM overlay system, protection assurance for P2p feature streaming, and SIP-flagging convention. A points of interest of proposed SALMON construction modeling with security, burden adjusting, and solidness are exhibited in Section 3. Area 4 depicts reproduction tests for SALMON and their execution results for P2p.

(iv) Shorter Service Delays. Clients may appreciate quickly switching distinctive P2p VIDEO-STREAMING channels over P2p systems and endure a noteworthy feature exchanging postponement and bigger playback slack, so our proposed SALMON gives not just a peer's agile leaving strategies acknowledged by SIP conventions, additionally an aforementioned dependability advancement for peers' joining and leaving to minimize normal administration delay from a client churn.

2. Related Work

As we know a coherent topology connected in present P2p feature streaming innovations is generally characterized into tree, network (i.e., various trees), and half breed of tree and cross section [12]. Despite the fact that tree-based P2p structure jam effortlessness, it is powerless against peers' flow of heterogeneity and beat. Cross section based P2p structure enhances a versatility to a flow from companions, however it safeguards more unpredictable associate association relations. In this paper , we embrace tree- based, instead of lattice based, P2p building design in proposed SALMON to cost-viably accomplish low administration latency, security procurement, and security for P2p feature streaming clients beat over Internet.

We quickly audit related works in proposed answers for build an application-layer multicast overlay system with security insurance, burden offering, and steadiness for versatile P2p feature streaming administration.

2.1. Application Layer Multicast (ALM). It is an application-level traversal technique for IP multicast parcels without an assistance from switches through unicast burrowing. ALM is likewise called as a practical device to build overlay systems for substantial scale Internet media applications. ALM has a points of interest of less overhead of support than switches, procurement of much bigger multicast bunches than IP multicast, less similarity issues than IP multicast and, simpler expansion to new peculiarities like security, lapse control, soundness, etc.

Since switches normally impair sending IP multicast bundles to keep a flooding of multicast information, relationship toward oneself calculations for viable transmissions in coherent topology of multicast overlay system turn into a key of ALM instrument.

As indicated in Fig 1(a), a solitary tree ALM means to give best-exertion single-source information streaming with an improvement of diminished inactivity and misfortune rates. Case in point to join an ALM tree for streaming information, another part (i.e., multicast executor, MA,) should first associate with a catalog server, a meeting point to which each part MA must unite at a first time. At that point, it will have the capacity to get a part rundown to discover least round outing time(rtt) ,lossrate, or data transmission among existing accessible parts for a superior nature of media streaming administration from source ALM.

A lattice topology demonstrated in Fig 1(b) is connected to give data transmission expending distributed feature streaming with favorable element of abstaining from recreating gathering overseement crosswise over different (for every source) trees, and versatility of part disappointment . Contrasted and a solitary tree approach, a various tree methodology is more confused. In a low-defer high-transfer speed lattice called Fast-Mesh for shared live streaming is proposed. In this work, we propose a concentrated heuristic with complete cross section learning to minimize a most extreme deferral of all companions in a lattice. They show by means of reproductions that their answer can achieve a little normal deferral of 60ms to 100ms for hundreds companions in a lattice with a source datarate of 10kbps. In the analyses over an Internet over a few nations, an actualized Fast-Mesh still shows low postpone, extending from tens to 600ms with a little information source rate of 30kbps.

In our proposed SALMON, a solitary source ALM tree plot as petitioned its straightforwardness in a connected security insurance, as well as a tree modification in enhancement of both versatility and solidness for P2p VIDEO-STREAMING administrations. Also, a tree-based SALMON can likewise demonstrated normal administration delays for extensive scale peers and lessen a stream of control messages.

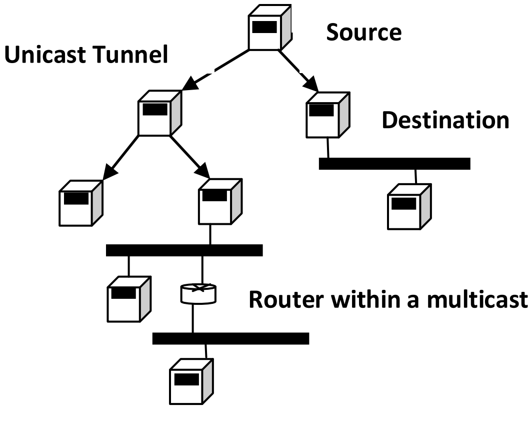
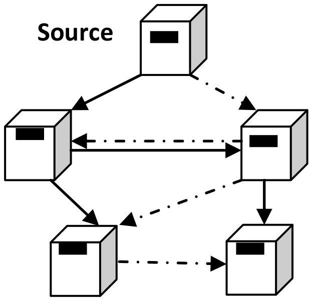


Fig 1.

a) Single-source tree



b) Single source Mesh

2.2. Privacy Protection for P2P video-streaming.

A security insurance of Internet feature streaming as generally done by symmetric encryption for less prolonged. There are two sorts of symmetric encryption instruments. One is a full encryption methodology; and other is specific encryption. For the most part, a primary burden of specific encryption is inadequate security and feature content ward. In difference, full encryption is frequently censured for a more drawn out figuring deferral which is not suitable for continuous feature streaming.

For a practical security insurance of ongoing feature streaming in P2p VIDEO-STREAMING, Advanced encryption standard (AES), which is a symmetric-key encryption standard is a most material strategy to secure voice information from meddler over the Internet. A standard involves three square figures, AES-128, AES-192, and AES- 266, embraced from an extensive accumulation initially distributed as Rijndael. Each of these figures has a 128-bit piece size, with encryption key sizes of 128, 192, and 266 bits, separately. Since AES is a symmetric crypto framework, it needs a key administration foundation to issue a typical session key (i.e discharge key) for later feature encryption/decoding in the middle of sender and recipient in P2p VIDEO-STREAMING. Three separate systems for a session key conveyance are preshared key, open key encryption, and a Diffie-Hellman (DH) key trade.

There is just a little measure of information that must be traded in a preshared key strategy. Be that as it may, it will make a versatility issue in vast gathering of conveying companions. An open key encryption can be utilized to make an adaptable protection security P2p VIDEO-STREAMING framework and generally obliges open key foundation (PKI) to appropriate open key. Its detriment is that expending a great deal more asset than a preshared key. For the most part, third technique for DH likewise has a versatility to ensure substantial scale P2p VIDEO-STREAMING administrations without a need of PKI. To ensure DH from man-in-a-center assault, validation in the middle of sender and beneficiary is required further. Thus, applying DH session key arrangement to secure P2P VIDEO-STREAMING administrations will expend more assets of transfer speed and reckoning than past ones yet without the need of concentrated PKI.

In SALMON, we utilize a mainstream altered DH called elliptic bend DH (i.e., EDH) key trade by means of SIP-flagging convention, since EDH saves a great deal less calculation overhead to build a safe multicast overlay tree for P2p VIDEO-STREAMING's privacy protection.

2.3. SIP Signaling for P2P VIDEO-STREAMING.

As demonstrated in Fig 2, SIP is a presently generally utilized flagging measures for Voip call setup and administration (e.g., enlistment, asset organization, status, and capacity trade). Session depiction convention (SDP) is SIP's convention to expressly introduce parameters of capacities connected in call setup and session administration, for example, a key trade data for arranging mystery key for DH flagging. ongoing convention (RTP) which is a decently characterized convention for conveying continuous media information like P2p VIDEO-STREAMING feature parcels.

As demonstrated in Fig 4, a choice k in SDP inside SIP can keep an open keys for DH motioning to arrange a typical discharge key for encoding a P2p VIDEO-STREAMING feature in RTP payload from source Multicast Agent (sma) to goal Multicast Agent (dma) Then, dma can utilize this basic mystery key to decode a scrambled RTP payload.

Since SIP with friend SDP not just can deal with a setup, change, and teardown of sight and sound session, additionally it upholds numerous augmentations, improvements, asset administration, and interworking with different heterogeneous frameworks, for example, protection assurance said above, exchanging data while continuous session, texting, et cetera, SIP is a best flagging convention over Internet for a control messages connected to outfit a proposed answers for security, burden adjusting, and strength in SALMON for versatile P2p VIDEO-STREAMING administrations.

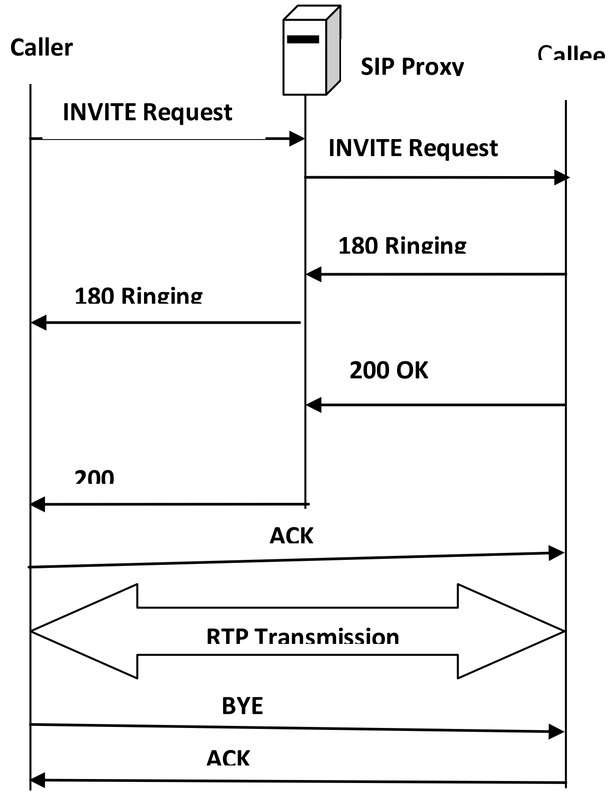


Fig 2. Operations of VoIP using SIP Signaling

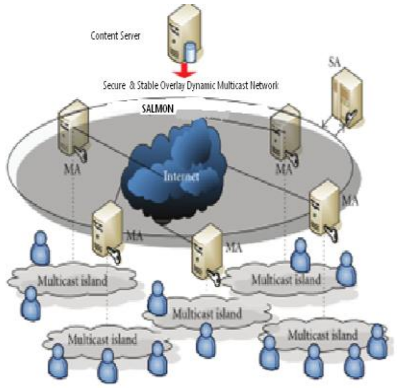


Fig.3 SALMON Architecture

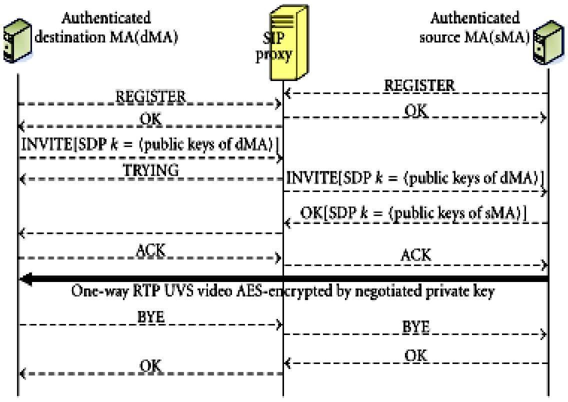

Authenticated destination MA(dMA)
SIP proxy
Authenticated source MA(sMA)
REGISTER
OK
INVITE[SDP k = (public keys of dMA)]
TRYING
REGISTER
OK
INVITE[SDP k = (public keys of dMA)]
OK[SDP k = (public keys of sMA)]
ACK
ACK
One-way RTP UVS video AES-encrypted by negotiated private key
BYE
BYE
OK
OK

Fig.4 DH(Diffe-Helman) Key negotiation via SIP/SDP Signaling

3. SALMON (Secure ALM Overlay with Load-Balancing and Stability for P2P VIDEO-STREAMING).

Utilizing SIP, SALMON is an overlay system comprises of a super operator (SA, i.e., meeting point) and distinctive Multicast Agents on diverse multicast islands over Internet to adequately give the P2p VIDEO-STREAMING administration for a devoted media source from substance server. SALMON's Multicast Agent are devoted machine frameworks or programming applications to get content information from source Multicast Agents, then multicast it to their nearby endorsers, or uncast it again to one or more other end of the line Multicast Agents over distinctive multicast islands as demonstrated in Fig 3. Moreover, SA won't just take an obligations to keep areas of Multicast Agents and a point by point topology data of SALMON additionally help to forward a feature from one source MA to goal MA, which was found in a private multicast island to finish a pervasive P2p VIDEO-STREAMING administration over a pervasive Internet. In any case, a topology of SALMON will change now and again on the grounds that an Internet clients can subscribe or unsubscribe a P2p VIDEO-STREAMING administration whenever, and a comparing Multicast Agent may join or leave a SALMON while possibly its nearby clients subscribe or no client subscribes a P2p VIDEO-STREAMING administration. Mean while, each dma in its multicast island may restores or jelly distinctive capacities of framework assets and outbound system transfer speed to forward a media content, so we propose a heap offering plan for SALMON to keep over-burdening sma from risking perceptual nature of P2p VIDEO-STREAMING administration for end peers.

3.1 Multicast Agent Joins/Leaves SALMON with Security Provision.

A system of another MA-joining SALMON is demonstrated in Fig 6 and portrayed as takes after.

(i) New MA meant as MAnew sends a SIP "REGISTER" demand with pointed out substance identifier and registration identifier to SA to approach SA for an association location of a leaf MA, to which a Manew can be joined and join a SALMON tree.

(ii) SA assumes a part of SIP substitute and database of SALMON topology data to send back a SIP "alright" reaction with SDP group of relating connection location of a leaf hub MA leaf, in which another Manewcan be joined with SALMON. Subsequently, a SA must keep up all state-of-the-art SALMON topology data to viably and accurately answer a right to gain entrance demand with a proficient leaf hub of taking care of a sending asked for feature to another supporter MAnew. That is a motivation behind why SA is known as a super executor .

(iii) After fruitful enrollment, MA new needs to set up an open parameters and key for a companion by EDH key trade calculation. Elliptic bend [9] capacity's parameter Eq1(a1,b1), base point G1= (x1, y1), and an arbitrary private key Knew are produced by MAnew. An, an open key Pnewcan be ascertained by knew, Eq1 and G1.

(iv) MAnew sends a SIP "Welcome" appeal message to remote Maleafvia SA substitute. SDP body in a SIP message incorporates an EDH open information of Eq1, G1, what's more Pnew.

(v) While MA leaf gets a MA new's "Welcome" message and MA new is approved to join a SALMON, it will arbitrarily produce a private key Knew and after that compute an open key Pleaf as per knew and get Eq1and G1. Also, a typical private key Kc for scrambling feature substance can be figured by kleaf, got Pnew, Eq1and G1.

(vi) Then MA leaf reactions a SIP "alright" message with SDP body including an open key Pleafback to MAnew.

(vii) While Manew gets an open key Pleaf from MA leaf's SIP "alright" message, MAnew can utilize Pleaf, private key knew, Eq1and G1to process a typical private key Kc for later decoding a scrambled feature.

(viii) Then, MAnew will send to MAleaf a SIP "ACK" message through SA to affirm a fulfillment of EDH key trade and a fruitful part join in SALMON. Then, SA can likewise upgrade its SALMON tree topology data of new member join as needs be While a nonleaf MA needs to leave SALMON after its neighborhood clients in multicast island consecutively unsubscribe a P2p VIDEO-STREAMING administration and it has no commitment to forward feature for different Mas (i.e., kid hubs of a leaving MA), a tyke hubs must reconnect to different Mas in SALMON to proceed with a P2p VIDEO-STREAMING administration.

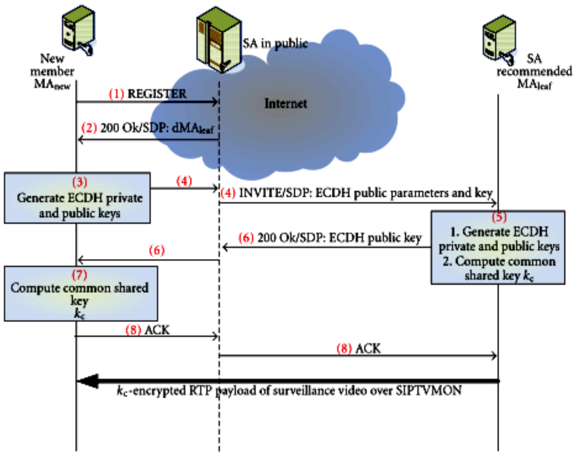

New member MA_{new}
SA in public
Internet
SA recommended MA_{leaf}
(1) REGISTER
(2) 200 Ok/SDP: dMA_{leaf}
(3) Generate ECDH private and public keys
(4)
(4) INVITE/SDP: ECDH public parameters and key
(5) 1. Generate ECDH private and public keys 2. Compute common shared key k_c
(6) 200 Ok/SDP: ECDH public key
(6)
(7) Compute common shared key k_c
(8) ACK
(8) ACK
k_c-encrypted RTP payload of surveillance video over SIPTVMON

Fig.5 SALMON's join procedure for a new MA

Such gracefully leaving procedures for a nonleaf MA_l leaving SALMON can minimize a P2P VIDEO-STREAMING service disrup tion from subsequent video packets loss for descendant nodes below a leaving node MA_l to maintain a overall quality of P2P VIDEO-STREAMING services for users.

Since all SIP messages including request and response in a previous procedures in new MA's join and old MA's leaving will be forwarded via a so-called SIP proxy ,these messages can easily help SA updating its SALMON topology information to cost-effectively Provide correct information upon later requests from SALMON members.

3.2 Optimizations for SALMON of Load Sharing and Stability.

P2p VIDEO-STREAMING is a close constant application administration, and a postponement demand is not as strict as feature conferencing and voice over IP. Along these lines, P2p VIDEO-STREAMING administration solidness is more essential than administration inactivity. As a SALMON's part MAs, which safeguard diverse abilities of framework assets and system transmission capacity, may join, leave, or fizzle in an overlay system of SALMON amid P2p VIDEO-STREAMING administration session, a shirking of P2p VIDEO-STREAMING administration interruption must be considered in proposed SALMON construction modeling. A bigger outbound connection transfer speed of Mas in Sp2p VIDEO-STREAMING- MON not just backings higher bit rate of P2p VIDEO-STREAMING feature, additionally more associations with remote dma with great nature of P2p VIDEO-STREAMING administration. In past scrutinizes [26, 26], an ALM tree's hub with more outdegree (i.e., higher data transmission) ought to be moved to a top of a tree to perform an advancement of burden imparting in overlay system to seek after better nature of administration.

Besides, an alternate imperative variable of improvement, which will influence solidness of SALMON, is client lifetime, on the grounds that Internet clients may join and leave P2p VIDEO-STREAMING administrations in diverse timing. To apply both elements said above, which may influence strength of overlay system, [26] utilizes a result of transmission capacity and life time that is Bandwidth and life-Time Product, for burden offering streamlining of overlay system. A Bandwidth lifetime item quality capacity is utilized as a measure to streamline an overlay system administration with low administration idleness and disturbance. Be that as it may, this capacity is so touchy it would be impossible a variety of data transmission on Internet to much of the time reproduce an overlay system.

We get BTP = data transfer capacity ×lifetime.

In this manner, it is proposed a further enhanced standard called normal transfer speed life-time item to viably minimize administration disturbance amid advancement for SALMON. An enhanced quality capacity of is characterized as takes after:

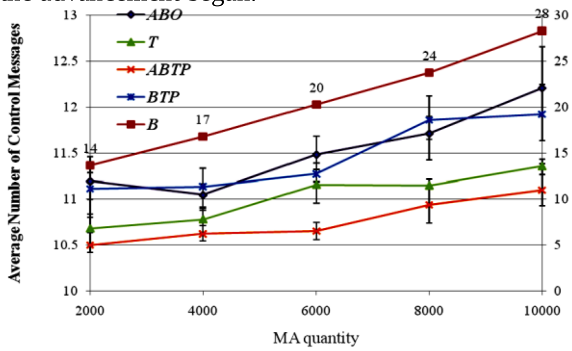
Avg Bandwidth life time Product

ABTP=$(\sum_{i-1}^{n} Bandwidth\ i\,)/n$ X lifetime .

4. Performance

The creation for SALMON utilizing Omnet++ , we recorded the check of control messages and administration interruptions, administration inactivity for distinctive advancement criteria. We performd each one experiment five times to discover the mean and standard deviation of these recreation results.

As demonstrated in Figure 6, ABTP paradigm beats less overhead of control message than the other four advancement criteria. Those criteria (i.e. B and ABO) without considering life time safeguard more control message. This is on account of more probability of abnormal state hubs leaving the SALMON tree showed more control messages are required to repair the SALMON for proceeding with OVERLAY DYNAMIC MULTICAST NETWORK administration, if MA's life time is not considered in streamlining for burden offering While an old MA leaving SALMON or SALMON's conformity for burden imparting, administration interruption may strike debase the nature of OVERLAY DYNAMIC MULTICAST NETWORK feature streaming administration for those dmas under isolates parent in SALMON. ABTP likewise safeguards less normal tally of administration disturbance to help SALMON to attain better nature of administration. Besides,abtp improvement model keeps lower profundities of SALMON tree than other criteria with the exception of experiment of MA amount 2000. Those improvement criteria without considering life time will keep less profundity than others in the vast majority of experiments To accept the perceptual nature of OVERLAY DYNAMIC MULTICAST NETWORK feature on SALMON, we assessed the parcel misfortune rates amid the administration disturbance in aforementioned recreations. At that point, the assessed parcel misfortune rates were connected to a recorded feature of around 2-moment length to measure the destination PSNR values as demonstrated in Figure 7. At the start of 10 to 20 seconds at the feature, because of the enhancement period was not begun yet, the tried feature protects more regrettable PSNR values than later periods after the advancement began.



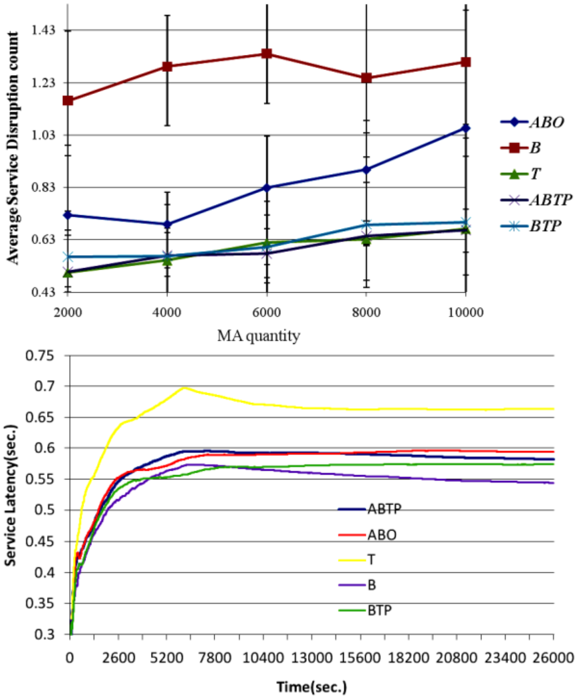


Fig.6 Average of Control messages,Disruption count,Service latencies

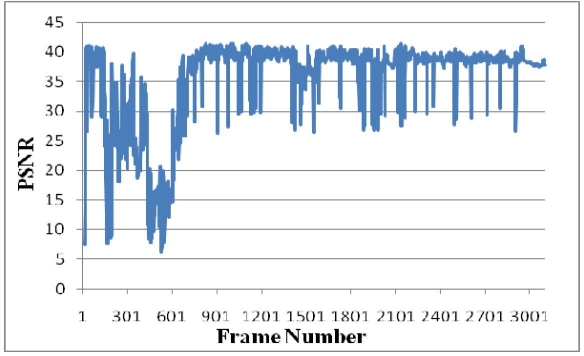


Fig . 7 PSNR values in SALMON

4. Conclusion

In this paper, It is suggested that a safe overlay system called SALMON utilizing application-layer multicast with burden imparting and security plans to cost-adequately give adaptable P2p VIDEO-STREAMING administrations for clients stir, for example, continuous joining and taking off. A proposed SALMON developed by SIP flagging can give adaptability to Internet clients with stable P2p feature streaming with protection protection, and a recreations results show that our SALMON's proposed advancement foundation considering a result of averaging transfer speed and life time in associates not just has a finer execution in overhead of control message, administration interruption, and administration idleness from tree Depth than other streamlining criteria additionally saves extremely adequate perceptual quality in goal PSNR values with security procurement.

We might likewise want to examine SALMON's dependability of open-circle and close-circle blunder controls, for example, peer's parcel reserve for versatile forward mistake remedy (FEC) and retransmission to further enhance P2p VIDEO-STREAMING's nature of administration over Internet.

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] 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

[4] 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.

[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] Tan G 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] http://www.planet-lab.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,

[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] Hellman M.E, "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 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]OMNet++, http://www.omnetpp.org/

[21]http://www.springerlink.com/content/v688368mu_017um6k/fulltext.html

[22] P. Francis, “Yoid: Extending the Internet Multicast Architectuire,” http://www.icir.org/yoid/