Integrated Approach for Multicast Source Authentication and Congestion Control

Karan Singh* and Rama Shankar Yadav

CSED, MNNIT, Allahabad, U.P., India
School of I.C.T., Gautam Buddha University, Greater Noida, India
karan@gbu.ac.in, rsy@mnnit.ac.in

Abstract. The coming age is information age in which data is being transmitted from network source to destination using unicast and multicast. Multicast services are very popular for transmission of huge information. Therefore, multicast network are growing day by day and it faces various problems such as reliability, security, congestion, connectivity scalability, fairness etc., due to exponential increment of network. Multicast Congestion is very serious problem to decrease the network utilization if network is not secure then condition may be worst and it is difficult to handle the situation. In this paper, we are providing secure multicast congestion control mechanism. In this mechanism global and local approach is proposed which provide the secure information in presence of congestion at minimum or any cost.

Keywords: Computer Network, Multicast Communication, Congestion Control, Source Authentication, Attack, Congestion Control, Security Goal, Layer System.

1 Introduction

Computer Network is essential part of our daily life. We perform various tasks such as email, newsfeed, stock information, IP TV, video conference etc. that use the unicast, broadcast and multicast transmission technology. In case of multicast huge amount of data is transfer from one computer to group of computer whereas it is efficient then unicast and broadcast but the design architecture raise various problem such congestion [1], security [12], fairness [2], reliability [17] etc. In case of congest network performance is decreased due to packet loss. So, each layer has different and independent authentication tree as well as signatures. Each receiver receives packets from joined layers then it verify the signature (reference signature is decrypted using public key known to receiver resulting to digest for the signature) now it compute the digest of received message using same hash algorithm as used at the sender side. If both digests matches, the received message is authentic. Besides of security mechanism for authenticity of source, the receiver performs the operations to maintain the desired performance and overload due to congestion in the system. The

* Corresponding author.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 16–30, 2013.

source S generates signature, computes authentication tree and generates packets of 3 independent layers [11, 20].

We can observe from figure 1 that the colors black, green and blue define for base layer (L_0), enhance layer 1 (L_1), enhance layer 2 (L_2) respectievely. The packets generated on different layers are of same color. Source sends packets with authentication information (hashes) from authentication tree in each layer independently. So, here is one authentication tree of each layer for one block (depend upon proposed approach). The receiver can join or leave the layer according to its own capacity or congestion situation. There are 3 receivers R_1, R_2 and R_3 whereas receiver R_1, R_2 and R_3 have joined layers (L_0, L_1, L_2), layers (L_0, L_1) and layer (L_0). The next section discusses the constraints behind integrated security aware multicast congestion control approach for multicast communication.

1.1 Constraints while Integration

The source equipped with the security mechanism send group of packets rather than a single packet and the level of security depends upon the random behavior of attacker. In other hand, multicast congestion control approach uses multiple layer joining and adaptive deaf period concept for leaving layer. Security mechanism provides the authenticity while it increases the communication overhead which may be the reason behind congestion problem. In other hand, congestion control manages the overhead but it may create problems (such as packet during deaf concept) for security mechanism. Thus security mechanism and congestion control are orthogonal issues, so there can be many constraints during integration which create open ended question disused in figure 1.

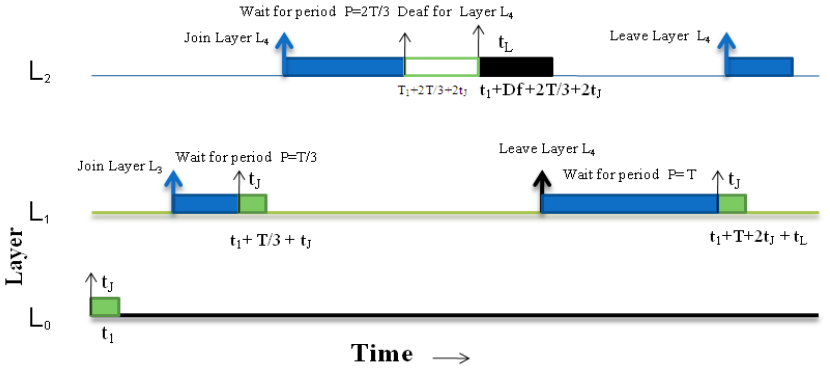

Fig. 1. Layer Deaf and Leaving Approach

In others case, figure 2 shows the deaf and leaving approach where base layer is L_0 (Black color, enhance L_1 (green color) and enhance L_2 (blue color) represented by line while box (, , and) are represented for joining overhead, leaving overhead, deaf overhead and decision period respectively. Suppose R_1 join

the layers L_0 , L_1, L_2 according to proposed method. At $t = t_1 + \frac{2T}{3} + 2t_J$, the receiver is overloaded and become deaf for the higher layer (L_2).

It can be observed that packets are lost when receiver is either overloaded or deaf for higher layer. Due to the lost packets the required secure information for such pakets are also lost. The chain could be break due to the congestion or loss in the secure information. At this stage the authenticity of the received stream is a major concern due to overloading or deaf decision.

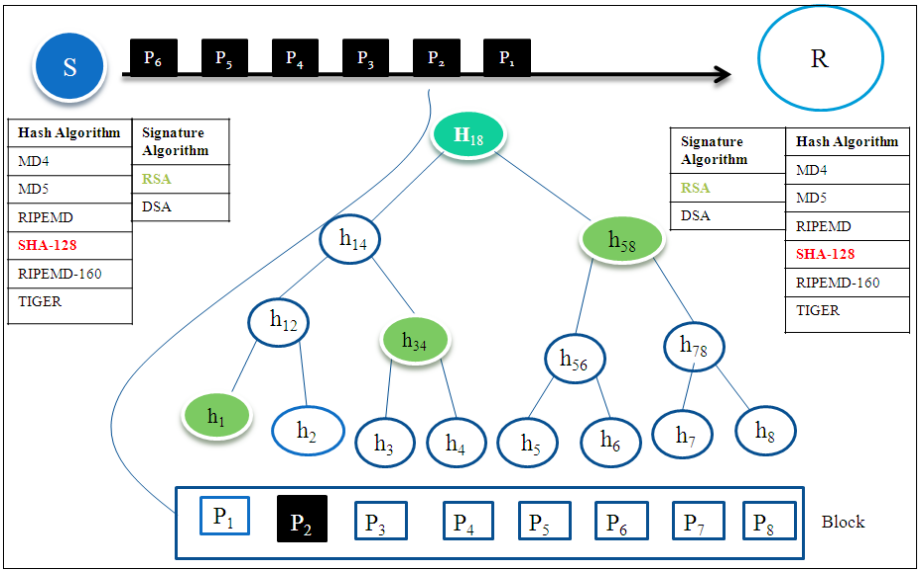

Fig. 2. Packet with Secure Information in a Layer

The communication overhead of packet in a layer depends upon number of hashes attached with packet, overhead of hash algorithm used, overhead of signature algorithm used. For example, we can see figure 2 where source is sending packets of base layer (L_0) to receivers. The hash values h1, h2, h3… h8 are computed by sender corresponding to packets P1, P2, P3.... P8 using hash algorithm and signature are generated by signature algorithm.

Here one source S is sending packets with secured information (number of hashes regarding hashes, for example secure information of P2 is h1, h34 h58) to receiver. It can be observed that more number of hashes, signature and increment in security level (to generate hashes) will create the communication overhead. Thus, on tuning with increased security level, hashes may lead to overloading and more packet loss. So, more attack probability leads to more congestion, more packet loss provide more security threats. It is a big challenge to manage the effect of increasing security overhead on overloading.

The tuning with increased security level, hashes may lead to overloading.

2 Related Work

2.1 Multicast Congestion Control

Computer networks uses the channels for transmit the data from source to receivers. If source rate increases the capacity of channel then congestion occur [7]. There are various multicast congestion control algorithms viz. RLM [4], TFMC [9, 10], FLID-DL [2], RLC [13], WEBREC [9], QIACCRM [5], EJLRDMC [11] etc. which control only the congestion and do not address the security threat. A few algorithms of congestions are describe as follows:

Receiver-driven Layered Multicast is the first well-known end to end congestion control for layered multicast. In RLM, receiver detects network congestion when it observes increasing packet losses. Receiver reduces the level of subscription if it experiences congestion. In the absence of loss, the receiver estimates the available bandwidth by doing the so-called join experiments when the join-timer expires. A join experiment means that a receiver increases the level of subscription and measures the loss rate over a certain period. If the join-experiment causes congestion, the receiver quickly drops the offending layer. Otherwise, another join-timer will be generated randomly and the receiver retains the current level of subscription and continues to do the join experiments for the next layer once the newly generated join-timer has expired.

Efficient Joining and Leaving for Receiver Driven Multicast Congestion Control (EJLRDMC) [11] have provided efficient layer joining and leaving through multiple layer joining and deaf leaving mechanism respectively.

Thus, we can see if source, router or receivers are working as a attacker then congest may increase more and network utilization will decrease so we need such type of mechanism which provide the authenticity of source and receivers. In next section we are providing secure multicast scheme to control the misbehavior of attack on system.

2.2 Multicast Source Authentication

Multicast source authentication provides [15, 16] the authenticity of sender to all receivers. This section is providing various types of secure multicast communication scheme which protect the network with security services such as authentication, Non-repudiation, Integrity etc. It divides the stream into blocks and embeds in the current block a hash of the following block. In this way, sign only the first block and then the properties of this single signature will propagate to the rest of the stream through the hash chaining .It is Off-line because entire stream is known in advance and this solution is not for fault tolerant.

EMSS [21] provides more or less probabilistic guarantees that it remains a hash-chain between the packet and a signature packet, given a certain rate of packet loss in the network. The robustness of the protocol to packet loss is proportional to the redundancy degree, k. In order to assure authentication of the stream, the sender continuously sends periodic signature packets .To verify authenticity of received

packets, a receiver buffers received packets and waits for their corresponding signature packet. The signature packet carries the hashes that allow the verification of few packets. These latter packets carry, in turn, the hashes that allow verifying other packets, and so on until the authenticity of all received packets is verified.

In second approach, packet are sending the same things (key, hash value, hash chaining) with a block of packet. But in this approach main problem will come after packet loss. If at any packet or block, the approach fails, the packet loss should not exceed the threshold limit.

Hash chaining scheme can't tolerate packet loss and the receiver cannot verify authenticity if any future packet once any portion of data is lost in transit. He Jin [19] approach uses the hash tree for decreasing receiver's computation overhead and authenticity because one root hash has the all value of leaf hash. Hash chaining is used for decreasing communication overhead and signing. It has the very less computation overhead because no need to compute more than one time at receiver side to verify the authenticity. It has some more communication overhead.

Adaptive Multicast Source Authentication (AMSA) [20] provides the mechanism to authenticate the source in multicast environment efficiently. This approach is like the tree approach where authentication information has sent with digest value from root of tree to leaf to all receivers where root digest is signed by source only one time in one block.

If we are increased security level, hashes may lead to overloading and more packet loss. So, more attack probability leads [8, 14] to more congestion, more packet loss provides more security threats. The situation will be worst. In next section, we are providing our proposed mechanism to tackle such type of situation.

3 Proposed Work

The global approach leads to higher level of overhead and affect congestion adversely. Thus, it forces the receiver to go for either leaving, deaf or join operation more frequently and deteriorating the situation more and more overhead. In localized storage approach decision about amount of information to be preserved is based on the availability of information with its successor multicast group in multicast hierarchy. At the local level the highest layer subscriber store the reference authentication among the group. The subscribing node retains the authentic information with intimation predecessor node (multicast node). For example, according figure 3 the group manager G provides availability of layer to subscribing nodes R_1, R_2 and R_3. Here R_3 subscribe the base layer L_0 whereas layers L_0, L_1 and layers L_0, L_1, L_2 are subscribed by R_2 and R_1 respectively.

Further, information stored at group managers lying at same level is also, local and its global one is store in its predecessor. Suppose receiver R_2 suffers from packet loss and switch to deaf or leave operation for layer L_2 (higher subscribed layer by receiver R_2). Later on either it resumes from deaf or join layer L_2 and requires authentic information, For authentic information it contact to group manager.

Table 1. Authentic Information of Layers for one Block

Layer	Block ID	Bundle ID	Packet in Bundle	Hash Vales
L_0	B_0	BUN0	P_1	h_2, h_{34}, h_{58}
L_0	B_0	BUN1	P_3, P_4	h_1, h_4, h_{58}
L_0	B_0	BUN2	P_4, P_5, P_6, P_7	h_3, h_{12}, h_8
L_0	B_0	BUN3	P_8	h_7, h_{14}, h_{56}
L_1	B_0	BUN0	P_1	h_2, h_{34}, h_{58}
L_1	B_0	BUN1	P_3, P_4	h_1, h_4, h_{58}
L_1	B_0	BUN2	P_4, P_5, P_6, P_7	h_3, h_{12}, h_8
L_1	B_0	BUN3	P_8	h_7, h_{14}, h_{56}
L_2	B_0	BUN0	P_1	h_2, h_{34}, h_{58}
L_2	B_0	BUN1	P_3, P_4	h_1, h_4, h_{58}
L_2	B_0	BUN2	P_4, P_5, P_6, P_7	h_3, h_{12}, h_8
L_2	B_0	BUN3	P_8	h_7, h_{14}, h_{56}

The authentic information preserved on R_1 to R_3 are termed as local one whereas global information is preserved at group manager store the authentic information for block B_0.

Table 2. Terms Used

Terms	Explanation
G	Group manager
LG	Local Group
RR	Requesting Receiver
n_i	Number of layers available
n_r	Number of receiver in group
n_o	Number of level in hierarchical multicast architecture to access the authentication information between path RR to GM or S
M	Number of hashes in one block
SL (R_i)	Subscribe layer by receiver (R_i)
Max_SL (R_i)	Maximum subscribe layer by receiver (R_i)
Comp_MSL (G)	Computed maximum subscribe layers by receiver (R_i) in group G
ADD_R	Address of receiver
CO	Communication overhead (time take by RR to node) between RR to node (which have stored the authentic information) to access the reference authentic information
N_AI	No. of Authentic Information stored at node for one block

The group manager intimate R_2 that requires information is available with receiver R_1 of the multicast group of R_2. Thus, R_2 get authentic information within local group.In this case required information stored at group manager is for layer L_2

which is highest available as well as subscribed layer available at this group manager. The detailed required information to be stored for layer L_0, L_1 and L_2 for one block (first block) are given in table 1. The information managed at group manager is for a block at time. That is block B_0 information are replaced by block B_1 and so on. The proposed approach is summarized in form of algorithm 1.

The effectiveness of proposed localized based authentic information can be used in the example shown in figure 3. Here, topology has seven routers (RT1, RT2, RT3, RT4, RT5, RT6 and RT7) and there end receivers are connected to end router (G) which is RT7. The topology is considered as hierarchical architecture. The table 3 is showing storage of authentication information of one block in global and local approach when source is sending packets with authentic information through path S->RT1->RT2->RT7->R1 or R2 or R3. It can be observed from table 3 that local approach required less authentication information storage then global approach.

Algorithm 1. *Localized based authentic information preservation*

1. For i= 1 to n_i

2. For i= 1 to n_r

Max_SL(R_i) = 0 // *Initially no layer is subscribed*

Comp_MSL(G) = Max(SL(R_1), SL(R_2),…… SL(R_{nr}))

3. For (I = 1 to n_r)

While (SL (R_i) ≤ n_i)

DO (operation)

Case: Operation =Join

Contact to G for authentic information

If (required information is available with group)

i. Provide it to RR

Else

i. Provide ADD_R in LG of RR where information is available

ii. Receiver gets information from local receiver

iii. SL (R_i) = {New SL } U {Already SL}

iv. Comp_MSL(G) = Max (SL(R_1), SL(R_2)…… SL(R_{nr})

v. remove authentic information for layer whose number is less than Max_SL (G)

break;

Case: Operation =Leave

i. SL (R_i) = {Already SL } - {Leave Layer}

ii. Comp_MSL (G) = max (SL (R_1), SL(R_2),…… SL(R_{nr}))

iii. add authentic information to the group manager

break;

Case: Operation = Deaf_ resumption

i. Contact group manager for authentic information

If (required information is available with group)

i. Provide it to RR

Else

i. Provide ADD_R in LG of RR where information is available

ii. Receiver gets information from local receiver

Break;

The significant meanings of symbols are given in table 2. Here, in global approach one block information of one layer preserve at source is 12 (3+3+3+3=12) hashes, so for 3 layer it store 36 (12*3=36) hashes at source.

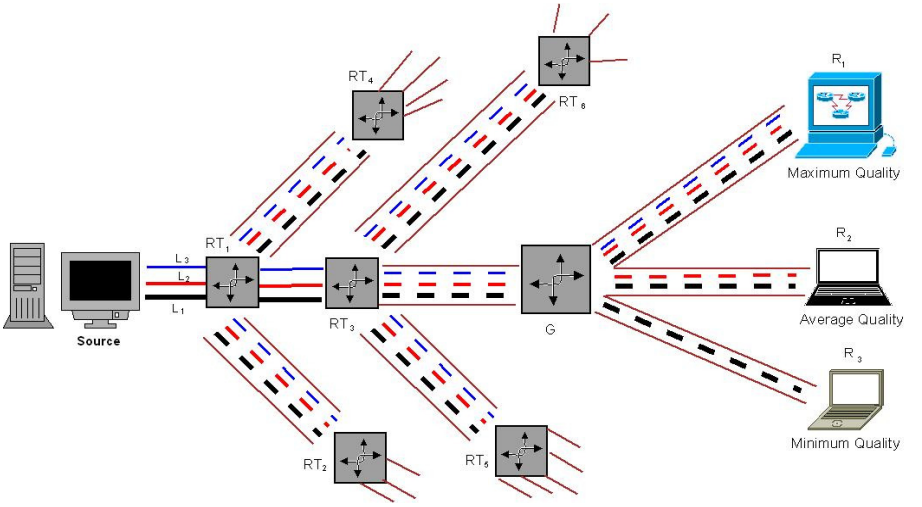

Fig. 3. Network Topology

On the other hand,each receiver store the one reference value of each layer to verify the packets i.e. 3 layer store the authentic information at all receiver which is 9 (3*3=9) hashes. Thus, total required store authentication information at all receivers are 45 (36+9=45) hashes. In other case of local approach the required authentication information for one block is stored at local group manager (only highest layer authentic information for one block i.e. 12 hashes) and maximum subscribe receiver (store all subscribe layer authentic information except highest layer i.e. 12*2=24) while receivers R_2, R_3 store the one referance authentic information for each layer (3*2=6) and R_1 store only one reference authentic information of highest layer.

Thus, total required stored authentic information at group and all receivers are 43 (12+24+1+6=43) hashes. However, storage of authentic information of localized based approach less than global based approach i.e. 2 hashes (45-43=2). For example number of layer (n_i) is 4 and number of receiver is 100 while maximum subscribe layer 4.

Table 3. Storage at node according to layer

Global Approach			Local approach		
Node	**Layer**	**N_AI**	**Node**	**Layer**	**N_AI**
S	L_0	12	S	L_0	0
S	L_1	12	S	L_1	0
S	L_2	12	S	L_2	0
RT_7	L_0	0	RT_7	L_0	0
RT_7	L_1	0	RT_7	L_1	0
RT_7	L_2	0	RT_7	L_2	12
R_1	L_0	1	R_1	L_0	12
R_1	L_1	1	R_1	L_1	12
R_1	L_2	1	R_1	L_2	1
R_2	L_0	1	R_2	L_0	1
R_2	L_1	1	R_2	L_1	1
R_2	L_2	1	R_2	L_2	1
R_3	L_0	1	R_3	L_0	1
R_3	L_1	1	R_3	L_1	1
R_3	L_2	1	R_3	L_2	1

In other case, for example shown in figure 3 where source is sending packets with authentic information through path S->RT1->RT2->RT7->R1 or R2 or R3. Suppose, communication overhead of nodes (request time to reach one node to other node) is equally distributed i.e 10 µs then communication overhead of request receiver (RR) to destination are illustrated by table 4. Here, in global approach for joining or deaf operation receivers send the request to source for access the reference authentic information of one layer, so these take 40 µs (10*4=40) communication overhead.

In other hand each receiver send the request to access the authentic information to a group manager if available or it provides the address of the receiver in the local group, so receiver take 10 µs (in best case) or 20 µs (in worst case) communication overhead. The communication overhead of requesting receiver (RR) is same bath approach i.e. 10 µs because receiver send to leaving request to group manager. It can be observed from table 4 that in deaf or join operation GBA communication overhead is 20 µs (40-20=20) more than LBA in worst case while LBA communication overhead is 30 µs (40-10=30) less than GBA in best case. Thus, receiver can access the reference authentic information while it performs join operation, deaf operation. Local based approach provide better performance than global based approach.

The communication overhead $CO_{iro} = \sum_{r=1}^{r=Rn} n_r \sum_{o=1}^{o=RT_N} n_o * CO_{111}$ where CO_{111} is communication overhead of one receiver to communicate first level node for only one layer authentication information and description of n_i, n_r, n_o are given in table 2.

At this cost (communication overhead) receiver access the authentic information in network overload situation and it verify the genuinity of source while performing the overload management operation.

Over the above provided secured information available irrespective of switching a receiver into deaf or leaving a layer on the occurrence of congestion. Up to now we have considered that intensity of attack is same all the time. However, in case intensity of attacker varies with time more prompt hash technique is required to apply.

Table 4. Communication overhead between RR to node

Global Approach				Local Approach				
Operation	**RR Node**	**Layer**	**CO (µs) (Worst)**	**Operation**	**RR Node**	**Layer**	**CO (µs) (Best)**	**CO (µs) (Worst)**
Join	R_1	L_0	40	Join	R_1	L_0	10	20
	R_1	L_1	40		R_1	L_1	10	20
	R_1	L_2	40		R_1	L_2	10	20
	R_2	L_0	40		R_2	L_0	10	20
	R_2	L_1	40		R_2	L_1	10	20
	R_3	L_0	40		R_3	L_0	10	20
Leave	R_1	L_0	10	Leave	R_1	L_0	10	20
	R_1	L_1	10		R_1	L_1	10	20
	R_1	L_2	10		R_1	L_2	10	20
	R_2	L_0	10		R_2	L_0	10	20
	R_2	L_1	10		R_2	L_1	10	20
	R_3	L_0	10		R_3	L_0	10	20
Deaf	R_1	L_2	40	Deaf	R_1	L_0	10	20
	R_2	L_1	40		R_2	L_1	10	20
	R_3	L_0	40		R_3	L_2	10	20

4 Results and Discussion

In this section simulation has been carried out to evaluate the performance of the proposed global and local level approach. The key parameters for performance measurement are stored authentic information, computation time, verification time, authentic packet ratio and throughput.

The effect of variation of block size, number of receivers, number of layers, deaf duration etc. are over these key parameters. The legends used in this section are listed in the table 5. The next subsection briefs about experimental setup used.

Table 5. Storage at node according to layer

Legends	Expanded form of legends	Description of legends
GBA	Global Based Approach	Receiver access the reference authenticates information from global level.
LBA	Local Based Approach	Receiver accesses the reference authenticate information from global level.

4.1 Experimental Setup Used

The simulation experiment has been carried out on Intel Core 2 dual processor 2.0 GHz, 3.0 GB RAM, 80 GB HDD machine supports with network simulation version 3.0 under Linux operating system. In this simulation topology the key component are sender (where message has been originated) and end router where multiple receivers are connected multicast. The roll of the intermediate router is to perform more routing decision and provide the authentic information to successor node. End router maintain multicast group and provide the authentic information a global as well as local level where as receivers stores regarding authentic information, computes the hashes and verify the genuinity.

On the others hand source compute hashes, make a bundle from packet and send it end router, from it is delivered to the multicast receivers. We have implemented the example figure 2 as simplest topology which is simplified form of multicast system in figure 3. It gives routers, source (sender) and multicast receivers. The network is heterogeneous in term bandwidth uniformly distributed in range (10-100) MBPS. The buffer used at each receiver is 100KB. The other simulation parameters are listed in table 6.

Table 6. Simulation Parameters

Parameter	Value used (fixed) (range)
Packet Size (Byte)	(256)(64, 128, 256,512,1024)
Hash Size (Byte)	(20)(16, 20,24,32)
Signature Size (Byte)	(128)(-)
Block Size (No. Packets)	(8)(2, 4, 8, 16,32)
Rate (Packet/Sec)	(10)(-)
Queue Size (No. Packet)	(100)(-)
Threshold (THARS)	5
Bundle size	(8)(1,2, 4, 8, 16,1)
Network bandwidth(MB)	(10-100)(-)
Link delay (ms)	(10-50)(-)

These values are same used in 11][12][13][20][21][22][23][25][28][30][31][36] [37] [38][40][42][48][44]. The next subsection deals with simulation results and it analysis.

4.2 Results and Analysis

The effect of variation of block size, number of receivers, number of layers, deaf duration etc. are over stored authentic information, computation time, verification time, authentic packet ratio and throughput. First we analysis the effect of variation in packet size followed by number of receivers.

Effect of Variation in Number of Level in Multicast Architecture

The effect of variation in number of level in multicast architecture on the joining overhead can be seen from figure 4. It has been observed that with increment in number of level in architecture then joining overhead increases and applicable for each one. This is because more the number of levels in architecture required more time to access this authentic information. The increment of local based approach is less than global one because in local based approach received the authentic information form group manager or neighbor receiver.

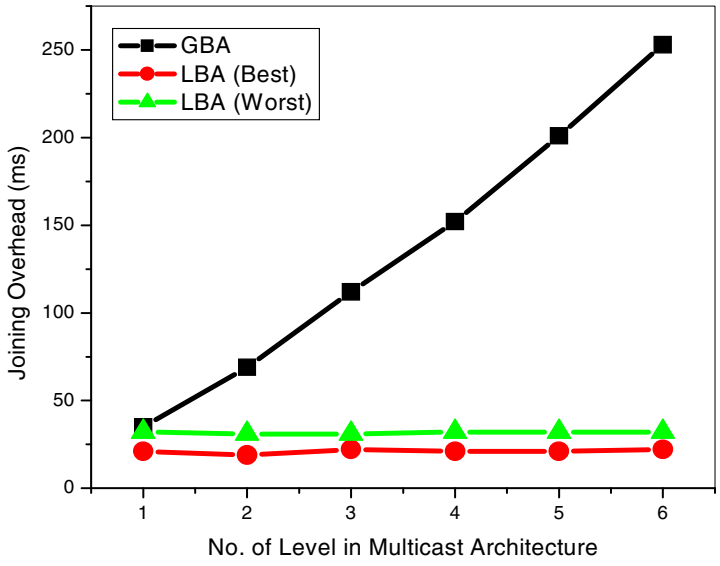

Fig. 4. Joining Overhead w.r.to No. of Level in Architecture

Effect of Variation in Number of Layers

The effect of variation in number of layer on the joining overhead can be seen from figure 5. It has been observed from figure 3 that with increment in number of layers increases the joining overhead which is applicable GBA, LBA (worst) and LBA (best)

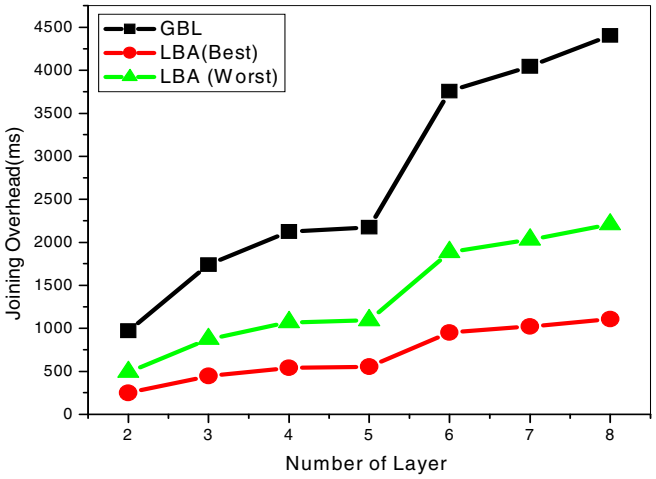

Fig. 5. Joining Overhead w.r.to No. of layer

approach. The reason behind increment in joining overhead is that receiver access more authentic information which take more time to access these authentic information.

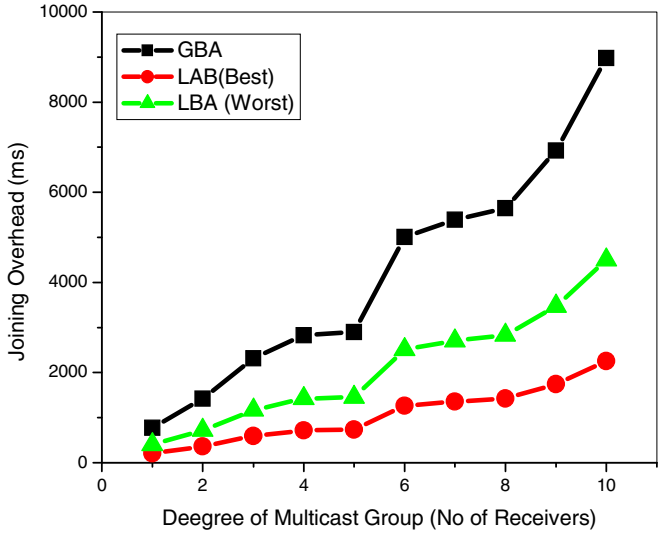

Fig. 6. Joining Overhead w.r.to degree of Multicast Group

In other word, it can be seen that increment in joining overhead of local based (LBA) approach is less than global (GBA) based approach. This is due to local based approach received the authentic information from local and it will take less time to access these information.

Effect of Variation in Number of Receivers

The effects of variation in number of receiver affect the joining overhead which can be seen from figure 6. It can be observed that joining overhead increases with increment in number of receivers in a group and this is applicable for all approach. However, lesser increment is observed for local approach as compared to global one.

5 Conclusion

In this paper, we proposed integrated security aware congestion control approach to improve the security of multicast system in presence of security threats. The proposed approaches provide the authentic information in layered multicast architecture for source authentication in presence of network overload. For this, we have proposed global based and local based approach. The aim of proposed work is to increase throughput and reduce the overhead to access the authentic information. The proposed global based approach (GBA) stores the authentic information at source end. When network is overloaded then receiver performs the deaf/leaving operation then authentic information of next successor packets is also lost. Due to this loss of authentic information, receiver is unable to verify the genuinity of source. So, the receiver receives authentic information from source at the cost of increased overhead. In local based approach (LBA) the group manager stores the authentic information stored at predecessor node and neighbor receiver. In case of overload, receiver will access the authentic information from predecessor node (best case) or neighbor receiver (worst case). The authentic information from layered multicast architecture is received when applying the overload management mechanism, the parameters such as level of architecture, number of layer and number of receiver which effect the joining overhead. The simulation results show that the joining overhead is less in LBA than GBA. The effectiveness of the proposed algorithm has been discussed through examples and extensive simulation results. The proposed security aware multicast congestion control approach increases the security and reduces the overhead in presence of security threats and network overload.

References

1. Yin, D.S., Liu, Y.H., et al.: A new TCPfriendly congestion control protocol for layered multicast. In: Proc. IASTED Conference on Internet and Multimedia Systems and Applications, Innsbruck, Austria (February 2006)
2. Byers, J., Frumin, M., et al.: FLID-DL: congestion control for layered multicast. In: Proc. NGC 2000, Palo Alto, USA, pp. 71–81 (November 2000)
3. Kulatunga, Fairhurst: TFMCC Protocol Behaviour in Satellite Multicast with Variable Return Path Delays. IEEE (2006)
4. McCanne, S., Jacobson, V., Vetterli, M.: Receiver-driven layered multicast. In: Proceedings of ACM SIGCOMM, New York, USA, pp. 117–130 (August 1996)
5. Johansen, S., Kim, A.N., Perkis, A.: Quality Incentive Assisted Congestion Control for Receiver-Driven Multicast. IEEE Communications Society ICC 2007 (2007)

6. Kammoun, W., Youssef, H.: An adaptive Mechanism for End-to-End Multirate Multicast Congestion Control. In: Proceeding of The Third International Conference on Digital Telecommunications, pp. 88–93 (2008)
7. Li, B., Liu, J.: Multirate video Multicast over the Internet: An Overview. IEEE Network (January/February 2003)
8. Bruhadeshwar, B., Kulkarni, S.S.: Balancing Revocation and Storage Trade-offs in Secure Group Communication. IEEE Trans. on Dependable And Secure Computing 8(1), 58–73 (2011)
9. Rizzo, L.: A TCP-friendly single-rate multicast congestion control scheme. In: Proc. ACM SIGCOMM, Stockholm, Sweden, pp. 17–28 (August 2000)
10. Floyd, S., Handley, M., Padhye, J., Widmer, J.: Equation based congestion control for unicast applications. In: Proc. ACM SIGCOMM, Stockholm, Sweden, pp. 43–56 (August 2000)
11. Singh, K., Yadav, R.S.: Efficient Joining and Leaving for Receiver Driven Multicast Congestion Contro. International Journal of Computer Applications 1(26), 110–116 (2010)
12. Singh, K., Yadav, R.S.: Overview of secure multicast Congestion Control. In: International Conference on Soft Computing and Intelligent Systems (ICSCIS 2007), Jabalpur (December 2007)
13. McCanne, S., Jacobson, V., Vetterli, M.: Receiver-driven Layered Multicast. In: Proceedings of ACM SIGCOMM (August 1996)
14. Athens/Glyfada, Greece, Replay Attack of Dynamic Rights within an Authorised Domain. In: Proc. of IEEE, Third International Conference on Emerging Security Information, Systems and Technologies (2009)
15. RFC 4046, Multicast Security (MSEC) Group Key Management Architecture (April 2005)
16. RFC-3740, The Multicast Group Security Architecture (March 2004)
17. Mokhtarian, K., Hefeeda, M.: Authentication of Scalable Video Streams With Low Communication Overhead. IEEE Trans. on Multimedia 12(7), 730–742 (2010)
18. Gorinsky, S., Jain, S., Vin, H., Yongguang: Design of Multicast Protocols Robust Against Inflated Subscription. IEEE/ACM Transactions on Networking 14(2) (April 2006)
19. He, J.-X., Xu, G.-C., Fu, X.-D., Zhou, Z.-G.: A Hybrid and Efficient Scheme of Multicast Source Authentication. In: Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. IEEE (2007)
20. Singh, K., Yadav, R.S., Sharma, A.K.: Adaptive Multicast Source Authentication. In: IEEE Proceeding of International Advance Computing Conference, IACC 2009, March 6-7 (2009)
21. Perrig, et al.: Efficient Authentication and Signing of Multicast Streams over Lossy Channels. In: IEEE Symp. Security and Privacy 2000 (2000)
22. Singh, K., Yadav, R.S.: Multicast Congestion Control in Adversary Environment. In: IPCSIT, vol. 31. IACSIT Press, Singapore (2012)