2012 International Conference on Industrial and Intelligent Information (ICIII 2012)
IPCSIT vol.31 (2012) © (2012) IACSIT Press, Singapore

Multicast Congestion Control in Adversary Environment

Karan Singh[1+] and Rama Sankar Yadav [2]

[1] School of I.C.T., Gautam Buddha University, Greater Noida, U.P., India

[2] Department of CSE, Motilal Nehru National Institute of Technology, Allahabad, U.P., India

Abstract. Computer network is essential part of our life which is used different technology to provide the services to users. Multicast is one technology which is mostly used for multimedia application but due to design architecture it suffer from congestion and un-security challenges. Many researchers are working in congestion control and some are providing solution for security issues in multicast. In this paper, we are providing a mechanism for congestion control while network is adversary. The proposed approach provides the secure information to receiver for authenticate to a source in presence of congestion at minimum or any cost.

Keywords: Authentication; Attack; Congestion; Multicast; Security.

1. Introduction

Computer Network is essential part of our daily life. We finished the many task 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 invite the 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) and compute digest of received message using same hash algorithm as used at sender side. In case both digest match the message received is said to be received from authentic source. Beside of security mechanism for authenticity of source, receivers perform the operations to maintain perform and overload (congestion) of system using multiple layer joining and deaf concept for leaving layers. We can observe from [11, 20] that S is source which generate signature, compute authentication tree and generate packets of 3 independent layers. In next section discusses the constraints behind integrated security aware multicast congestion control approach for multicast communication.

The security mechanism source send group of packets instead of sending one packet at a time and adjustment in deployed security level to incorporate the random behaviour of attacker. In other hand, multicast congestion control approach uses multiple layer joining and adaptive deaf period concept for leaving layer. Security mechanism provides [43] the authenticity while increases the communication overhead while it may be reason of congestion. 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 [19, 20, 21] and congestion control [3, 11, 18] are orthogonal issue so there are many constraints while integration which create open ended question which are disused below. 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

[+] Corresponding author. Tel.: Tel.: +911202346081
E-mail address: karancs12@gmail.com

loss provide more security threads. It is very difficult to manage the effect of increasing security overhead on overloading.

The rest of the paper is organized as follows. Section 2 deals with related work whereas section 3 details the proposed solution of our research and section 4 discussions with analysis of results. Finally, section 5 deals with concluding remarks

2. Related Work

2.1. Multicast Congestion Control

Computer network use the channels for transmit the data from source to receivers. If source rate increases the capacity of channel then congestion occurred [7]. There are various multicast congestion control algorithms for example RLM [4], TFMC [9, 10], FLID-DL [2], RLC [13], WEBREC [9], QIACCRM [5], EJLRDMC [11] etc. which only control the congestion but doesn't aware security threat. There are some algorithm which describe that they only control congestion and not working in distrust environment. There are following

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 provide efficient layer joining and leaving through multiple layer joining and deaf leaving mechanism respectively.

Thus, we can see if source, router or receivers are worked as a attacker the congest may be increase more and network utilization will decrease so we need the a such type of mechanism which provide the authenticity of source and receivers. In next section we are providing secure multicast scheme to controlling the misbehaviour 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 type 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 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 for the sender to continuously assure the authentication of the stream, the sender 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 we can sent 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 any packet or block loss the approach will fail, so packet loss should not exceed from threshold limit.

Hash chaining scheme can't tolerate packet loss and the receiver cannot verify authenticity if any future packets once any portion of data is lost in transit. He Jin [19] approach use the hash tree for decreasing re-

ceiver's computation overhead and authenticity because one root hash has the all value of leaf hash. Hash chaining use 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 the little more communication overhead.

Adaptive Multicast Source Authentication (AMSA) [20] have provide the mechanism for authenticate the source in multicast environment efficiently. This approach is tree approach where authentic 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 provide more security threads. The situation will be worst. In next section, we are providing our proposed to tackle such type of situation.

3. Proposed Work

Our approach is integration of source authentication mechanism with multicast congestion control where message are divided into blocks and one block is sending to receiver in form of group (bundle) of packets along with sibling hashes. Here, each receiver can perform join, deaf or leave operation to balance between congestion minimization and quality of services (QoS). The QoS is measured through throughput and security provided. While handling the congestion, it is to be noted that reference authentication information to be available or irrespective how much information are lost. The reference authentication information can be preserved at local as well as global level. For the case of global concept of preserving the authentic information the copy of information is preserved at source (originator of the layers) and on joining or resumption from deaf receiver is required to contact source.

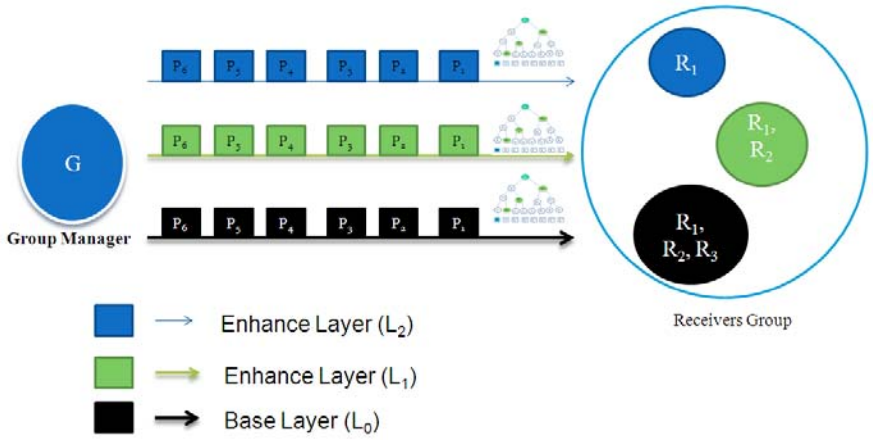

Fig. 1. Authentic Packet Receiving Process

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. The information managed at group manager is for a block at time.

The effectiveness of proposed localized based authentic information can be used in the example shown in figure 2. 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 authentication information of one block in global (GBA) and local (LBA)approach when source is sending packets with authentic information through path S->RT1->RT2->RT7->R1 or R2 or R3. It can be observed that local approach required less authentication information storage then global approach. 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.

In other hand each receiver store the one reference value of each layer for verify the packets i.e. 3 layer stored authentic information at all receiver is 9 (3*3=9) hashes. Thus, total required store authentication information at source and 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 referance authetic information of highest layer.

Thus, total required stored authentic information at group and all receivers are 43 (12+24+1+6=43) hashes. However, the storage for 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.

In other case, for example shown in figure 2 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.. 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.

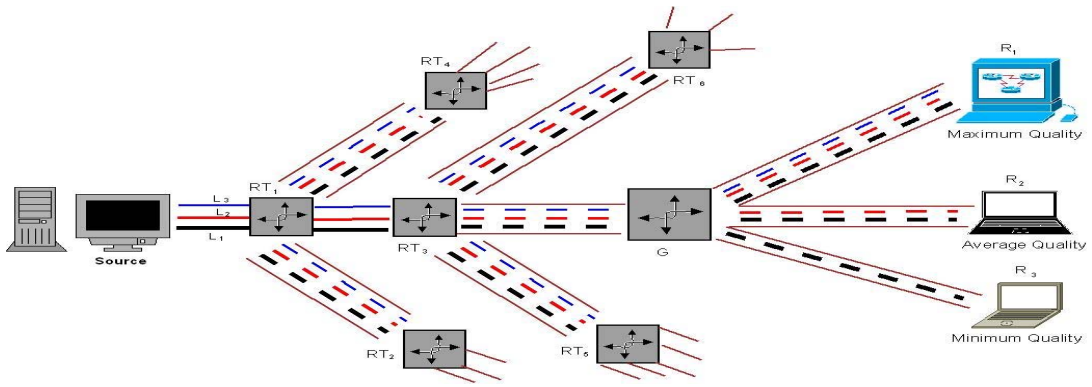

Fig. 2. Network Topology

In other hand each receiver send the request to access the authentic information to group manager if available or it provide the address of received in 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 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 perform join, deaf operation and local based approach provide the 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 . 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. The next scheme deals with adaptive security and overload management

4. Result 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 next subsection briefs about experimental setup used.

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 support 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 intermediate router is more perform 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. 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 1. These values are same used in [11][12][13][20][21]. The next subsection deals with simulation results and it analysis.

Table 1. Simulation Parameters

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

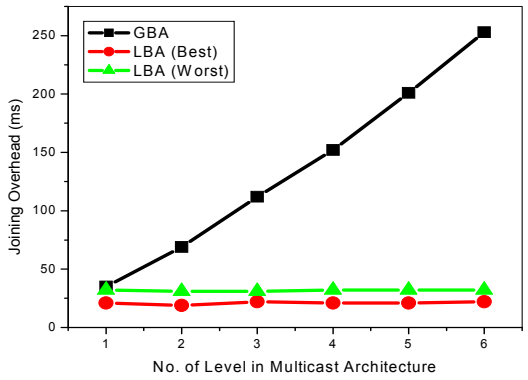

Fig. 3. Joining Overhead w.r. to No. of Level in Architecture

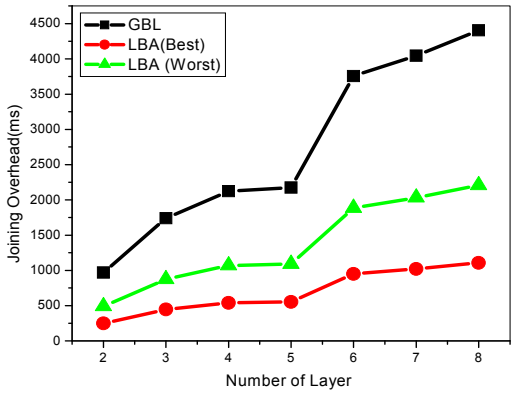

Fig. 4. Joining Overhead w.r.to No. of layer

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.

Figure 3 is showing the effects of variation in number of level in multicast architecture affect the joining overhead. The graph is showing that LBA (Best) have less joining overhead because it receives the authentic information from group members.

Effect of variation in number of Layers.

Figure 4 is showing the effects of variation in number of layers in multicast architecture affect the joining overhead. The graph is showing that LBA (Best) have less joining overhead because receivers have more choice to receive the authentic information.

5. Conclusion

In this paper, we proposed congestion control approach in adversary environment to improve the security of multicast system.. 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. 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. The simulation results show that the joining overhead is less in LBA than GBA. The effectiveness of the proposed mechanism 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.

6. References

[1] D.S. Yin, Y.H. Liu, et al..: "A new TCPfriendly congestion control protocol for layered multicast", in proc. IASTED conference on Internet and Multimedia Systems and Applications, Innsbruck, Austria, Feb. 2006.

[2] J. Byers, M. Frumin, et al., "FLID-DL: congestion control for layered multicast", in Proc. NGC2000, Palo Alto, USA, PP.71-81, Nov. 2000.

[3] Kulatunga, Fairhurst “TFMCC Protocol Behaviour in Satellite Multicast with Variable Return Path Delays” IEEE 2006.

[4] McCanne S., Jacobson V., and Vetterli M.: Receiver-driven layered multicast, Proceedings of ACM SIGCOMM, pp.117-130, August 1996, New York, USA.

[5] Stian Johansen, Anna N. Kim, Andrew Perkis.:“Quality Incentive Assisted Congestion Control for Receiver-Driven Multicast” IEEE Communications Society ICC 2007.

[6] W. Kammoun, H. Youssef “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] Bezawada Bruhadeshwar and Sandeep S. Kulkarni, “Balancing Revocation and Storage Trade-offs in Secure Group Communication” in IEEE Trans. on Dependable And Secure Computing, vol. 8, no. 1, pp. 58-73, Feb. 2011.

[9] L. Rizzo. “A TCP-friendly single-rate multicast congestion control scheme”, in Proc. ACM SIGCOMM, pp.17 – 28,Stockholm, Sweden, August 2000.

[10] S. Floyd, M. Handley, J. Padhye, and J. Widmer “Equation based congestion control for unicast applications” in Proc. ACM SIGCOMM, pages 43 – 56, Stockholm, Sweden, Aug. 2000.

[11] Karan Singh and Rama Shankar Yadav “Efficient Joining and Leaving for Receiver Driven Multicast Congestion Control” in International Journal of Computer Applications 1(26):110–116, February 2010.

[12] Karan Singh and Rama Shankar Yadav “Overview of secure multicast Congestion Control” International Conference on Soft Computing and Intelligent Systems (ICSCIS-07), Jabalpur, Dec 2007.

[13] McCanne, S., Jacobson, V., Vetterli, M.: Receiver-driven Layered Multicast. 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] Kianoosh Mokhtarian and Mohamed Hefeeda, “Authentication of Scalable Video Streams With Low Communica-

tion Overhead” in IEEE Trans. on Multimedia, vol. 12, no. 7, pp. 730-742, Nov. 2010.

[18] S. Gorinsky, Sugat Jain, Harrick Vin, Yongguang “Design of Multicast Protocols Robust Against Inflated Subscription” IEEE/ACM Transactions on Networking, Vol. 14 No. 2, April 2006.

[19] HE Jin-xin, XU Gao-chao, FU Xiao-dong, ZHOU Zhi-guo A Hybrid and Efficient Scheme of Multicast Source Authentication Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing IEEE, 2007.

[20] Karan Singh, Rama Shankar Yadav and Amit Kumar Sharma, "Adaptive Multicast Source Authentication " in IEEE proceeding of International Advance Computing Conference, 2009. IACC 2009, 6-7 March, 2009.

[21] A. Perrig et al., Efficient Authentication and Signing of Multicast Streams over Lossy Channels IEEE Symp. Security and privacy 2000.