International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1477-1482 www.ijaem.net ISSN: 2395-5252

The Pragmatic General Multicast (PGM)

Anshika Katiyar,
Student, Amity University(AIIT), Jaipur, Rajasthan

Submitted: 15-02-2022 Revised: 25-02-2022 Accepted: 28-02-2022

ABSTRACT: ThePragmaticGeneralMulticast(PGM)transportprotocolisadependablemulticasttransportmechanism. It is suitable for applications that are multi-receiver file transfer because it can reliably transfer asequence of packets to multiple receivers simultaneously. It provides best efforts over datagram services. It isaimed at applicationsthat need sequential, delicacy-freemulticastdata delivery.
PGMusesahybridtechniquethatincludessuppression, NAK[1]elimination,constrainedforwarding,andFECto achievescalability.PGMis capableofhigh-speedoperations,supportsAsymmetric Networks,[2] andachieveshigh networkutilization.
ThoughPGMisnotastandard yet,itisanIETFexperimentalprotocol,butisstill used inlotsofcommercialand educational settings, likenetworkingdevices suchasoperating systemslikewindows.

Still PGM is not perfect, In addition to usual end to end authentication vulnerabilities, PGM have other securityissues as well. This assignment provides basic information about the PGM, security issues with PGM and itsvulnerabilities,later wewillseesomeofthesolutionsforthesame.
Inthisassignment,wewillalsotouchonthearchitecture of PGM. In which we will see about Source functions, receiver functions and network elementfunctionsofPGM.

I. INTRODUCTION

The Pragmatic General Multicast (PGM) transport protocol is a dependable multicast transport mechanism. It issuitableforapplicationsthataremulti-receiverfiletransferbecauseitcanreliablytransferasequenceofpacketsto multiple receivers simultaneously. It provides best efforts over datagram services. It is aimed at applicationsthatneedsequential, delicacy-freemulticastdata delivery.
PGMiscapableofhigh-speedoperations,supportsasymmetricnetworks,anda chieveshighnetworkutilization.Itisbetter thanthetraditionalend-to-end protocols thatexploitInternetmulticast.
It have Acknowledgement (ACK) and Negative acknowledgement (NAK)[3] both, as an attempt to overcome thescaling and protocol reliability problems due to lousy IP networks. PGM makes sure either receiver receives allthe data packets or it detects unrecoverable lost data packets. The Pragmatic General Multicast (PGM) transportprotocolisadependable multicasttransportmechanism.

<u>MULTICASTPROTOCOLS:</u>

Networksemploymulticastprotocolstomakereceivingandrelinquishingmembershipinmulticastgroupseasier. Whenever there is one-to-many communications, then word multicast is used. Multitasking is atechnology that allows a single packet to be sent to many destinations. This is advantageous for bandwidthreduction,networkparallelism, and transmitter costreduction.

1. NAK:Negativeacknowledgment, Sent byreceiverstoaskforrepairs.
2. Asymmetric Network: A network has various routes for incoming and outgoing networktraffic.Assuchtraffictakesan alternateroutewhenenteringorleavingthenetwork.
3. An Acknowledgment (ACK) or Negative Acknowledgment (NACK) is a short message sentby the recipient to the transmitter to show whether it has accurately or erroneously got a datapackets,respectively.

<u>Reliable multicast:</u> the most well-known reliable transport protocol is TCP which makes sure sequential deliveryof data packets. But it is used for unicast transmission, not multicast, for multicast, such protocol does not existyet.
Byreliable wecan sayaprotocolthatiscapableof:
- Lossrecovery
- Noduplication
- Ordereddelivery
- Isolationofindependent failures

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1477-1482 www.ijaem.net ISSN: 2395-5252

Reliable multicast is getting more important every day as we need it in many applications nowadays like mediaconferencing.Becauseofthe demandfor

multicastcommunication,manyreliablemulticastprotocolshavebeenmade but although several protocols have been created, none of them are as reliable as TCP for unicasttransmission.

ManyprotocolsattemptedtoemulateTCP,inwhichthe receiverprovidesanacknowledgementafterreceivingthe data packet, with transmitting continued in the same manner as TCP, based on the results of the slowestreceiver.

Theproblemwiththistypeofapproachisthat itcancause themessage“implosion”.

A protocol reliability can be sender-initiated or receiver-initiated which means either sender or receiver will beresponsiblefor the detectionoflostdata packets(ifany).

Receiver-initiated reliability protocol: It requires receivers to detect if there is any loss of packets. The receivergenerates a negative acknowledgement (NAK) in case of loss of the packet. The packet can be retransmitted inresponse. There isalwaysa chanceofNAKimplosionif manyreceiverslosedata packets.

Therearemanywaystodealwithimplosionlikesuppressionmechanism,tominimizethe numberofduplicateNAK’s.

Advantages:morescalable,no ACK.

Disadvantages:complex,NAKimplosion,unlimitedbuffering.

Sender-Initiated reliability protocol: It requires the sender to detect any packet loss that may occur. A positiveacknowledgement is sent by the receiver on receiving the packet, if acknowledgement is not received the packetisconsideredlostandthepacketmayget retransmitted.

Advantages: simple and limited buffering.Disadvantage:ACKimplosion,scalability

There are many other reliable multicast protocols like SRM, RMTP, MTP-2, RAMP, TMTP, Log-based,

RMP.Multicastprotocolsessentiallyaredividedinto 2classes:

- Datareliabilityandordering,as wellascausation,inmulticastprotocols.
- Data-reliablemulticastprotocolswithoutorderingorcausation.

Protocols can also be different in terms of the logical structure of communication pathways, do they useACK/NAK or both, their design, receiver/sender reliability, etc. Several schemes were used to make multicastprotocolsmorereliablelikeimprovingscalabilityviahierarchyortryingNAKsuppression.[4]

A strategy for Negative affirmation (NAK) Suppression, the technique involving the meansof: verifying that a NAK should be transmitted; deciding whether data or other channelinformationat presentshouldbetransmitted over achannel; andtransmittingtheNAK

PGMPROTOCOLDESCRIPTION:

PGMisadependablemulticasttransportprotocol,aspreviouslystated.PGM wascreated withsimplicityinmind, and it achieves scalability with a hybrid method that incorporates suppression, NAK removal, limitedforwarding,and FEC.Hierarchyisconstructed usingPGM-capable NetworkElements.

PGM was designed to be compatible with non-PGM-based NE’s as well though with less efficiency when thenumber of PGM-based NEs is low, the PGM tree's fan-out increases, making suppression and FEC moreimportantinprovidingsomescalability.

PGM is compatible with networks that only offer multicast from sender to receiver since it works OK withreceivers that don't support multicast. It also makes optimal use of asymmetric networks by utilizingbackchannel and width, as asymmetric networks feature high capacity sender-to-receiver channels while havingconfined back-channels,i.e. fromreceiver tosender.

An examples of application that use PGM can be disk imaging, it does not wait for sluggish receivers to collectthe missingdatalaterusingtypicalclient-servertechniquesinthisapplication;instead,itjustcontinueswiththenewdata.

PGMFUNCTIONALITY:

- SourcePathEstablishment[5]
- NAKSuppression(referto footnote3)
- NAKElimination[6]
- NAK Anticipation[7]
- BasicDataTransfer
- RestraintConstraint[8]

assuming data and other channel data shouldn't be transmitted over the channel, in any casebuffering the NAK. The method of claim further containing the means of: deciding whether apredetermined number of NAKs have been buffered; and sending the NAKs of thepredeterminednumber.

4. Interleaved with ODATA, sources intermittently multicast Source Path Messages (SPM: Sentby sources: used to establish up turn around way from receivers to sources.) to set up sourcepath state for a given TSI in all

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1477-1482 www.ijaem.net ISSN: 2395-5252

PGM network elements and receivers on the distribution treefrom the source. SPMs are propagated PGM-hop by-PGM-hop from the source along thedistributiontreefortheTSI.

5. PGM network elements make Retransmit State for each NAK they get. The Retransmit Stateis related with the interface on which the NAK is sent. It records the TSI and SQN of theNAK alongside a list of the interfaces on which any occurrence of the NAK was gotten. Oncethe retransmit state exists for a given TSI/SQN, the PGM network elements affirm but dodon't forwardfurtheroccurrencesofthatNAK.
6. In expectation of response to and taking out copies of the NAK that might show up fromdownstream network elements build up a repair state without outgoing interfaces when hearsanupstreamNCF(NCF: SentbynetworkelementstoNAKers).

7. When a NAK is received, the source multicasts the mentioned retransmission (RDATA: Dataparcelsdetestfromasourcein answerto a NAK.).ThePGM networkelementsforward the

- Lossand DetectionRecovery[9]
- LocalRepair[10]
- TransmitWindowAdvancement[11]
- Options

RDATA provided that they have the relating Retransmit State and just on those interfaces inthe comparing interface list. Simultaneously, the PGM network elements dispose of thecurrentRetransmitState.

Upon receipt of a NAK, a source multicasts the mentioned retransmission (RDATA). TheRDATA packets have the very same format as ODATA packets, but they contrast in the typefield. Therefore, retransmissions only propagate across the network segments, which arrive atreceiversthatlostthe relatingtransmission.

8. A DLR is a committed host function configured to go about as a re-transmitter for chosenpackets in which it should likewise go about as a receiver. In response of the NCFs that it getsforthesechosen groups,itmulticastsarepeat of thatNCF withachoice givingitsown NLA.
9. Any receiver that gets a NCF for which it has the corresponding RDATA may multicast thatRDATA (following a random back-off), in this manner bringing about a lessening inretransmit latencyunderneath the pointoflocalrecovery.
10. Sources may advance the trailing edge of the window discretionarily. Executions mightuphold automatic adjustments like keeping the window at a fixed size in bytes or packets, orfixed real time duration. Furthermore they may optionally postpone window advancements inabsenceof NAKs.

II. ARCHITECTURE:

Because PGM is an end-to-end transport protocol, it specifies both sender and receiver packet formats andprocedures.ToincreasethedependabilityofNAKs and thetransmissionofrepairs,italsospecifiespacketformatsandproceduresfor networkelements.

This section explains how these functions are divided:SOURCEFUNCTIONS:

DataTransmission:

- ODATApackets[12]gets multicastbythesourcewithaspecific transmissionrate.

SourcePathState:

- SPM[13]s (Source path messages) are used to create a source path state, SPMs are transmitted withODATAtoestablishSPS(source pathstate).

NAKReliability:

- SourcesendsanNCF[14]onreceivingpackets,so ifiseasier to detectifanypacketislost.

Repairs:

- RDATA[15]aretransmittedbythesourcewhentheyreceiveNAKfordatasentwiththetransmitwindow.

TransmitWindowAdvance:

- Sources might propel the following edge of the window as per one of various methodologies.Automaticchanges,suchaskeepingthewindowataparticular sizeinbytes,aspecific number ofpackets, or a defined real-time length, may be maintained by executions. Furthermore, they MAYdeferwindowadvancesfor aperiodoftime ifNAK-silenceisdetected.

RECEIVERFUNCTIONS:

SourcePathState:

- When receivers need to ascertain the PGM network's last hop, they employ SPMs for each TSI towhichtheydirecttheirNAKs.

DataReception

- Duplicates needtobeeliminated,soreceiversuseODATAand findiftherearenyduplicates.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1477-1482 www.ijaem.net ISSN: 2395-5252

11. ODATA:Thispacketissentbytheserver/sourceonmulticastaddress.
12. SPM: Sentbysources: used to establishreversepath fromreceivers tosources.
13. NCF: Sentbynetworkelements toNAKers.
14. RDATA: Data packetsresentfromasource in replytoaNAK.

Repairs:

- If a data packet is lost, the receiver must continuously send NAKs until a matching NCF isreceived. The receiver unicasts NAKs to the final hop PGM network for data packets that weremissingfromthesequence(receiver canalsomulticastNAKs withaTTLof1tothelocalgroup).

NAKSuppression:

- During the back-off interval receivers suppress the NAK for which matching NAK/ NCF is alreadyreceived toavoidduplicity.

ReceiveWindowAdvance:

- IfaPGMdatapacket/SPMisreceivedwithinthetransmit windowandit movestothereceivewindow,the receiver advancestheir receivewindowinstantly.

NETWORKELEMENT FUNCTIONS:

SourcePathState:

- BeforemulticastingSPMsintheusual waynetworkelementsinterceptsSPMsandforeachcorrespondingTSIsuse themtoestablishthe sourcepathstate.

NAKReliability:

- For each NAK received network element send a NCF in response. A repair state is produced foreachNAKreceivedbynetworkcomponents, whichrecordsthetransportsessionidentificationandtheNAK'ssequence number.

ConstraintNAKForwarding:

- OnlythefirstcopyofanyNAKarerepeatedlyunicastforward bythenetworkelementsforantNAK they receive to until an NCF is received in response upstream PGM network node on thedistributionchannelfortheTSIWithaTTLof1,itmayalsomulticastthisNAK upstream.

NAKElimination:

- AlltheduplicateNAKareeliminatedbythenetworkelementforwhichtheyalreadyhavearepairstate, andthenitresponsewitha correspondingNCF.

ConstrainedRDATAForwarding:

- RDATAissenttointerfaceswhereuponthecomparingNAKwasreceived,networkelementsuseNAKstokeep upwiththe repair state comprisingoftheseinterfaces.

NAKAnticipation:

- • As soon as it hears an upstream NCF, it enters a repair mode without outgoing interfaces inpreparation of reacting to and deleting duplicates of the NAK that may arrive from downstreamnetworkelements.

III. SECURITYANDVULNERABILITIES WITHPGM:

PGMisstillanexperimentalprotocolandhave manyissues withsecurityas wellasgeneral,inthissection wewillsee problemswithPGM, aswellassecurityissuesfacedbyit.

- Networkelement memoryrequirements:IfaNEisusedinmanyPGM sessions,itmaynothaveenoughmemory to hold all of the outstanding NAKs from all of the sessions. As a result, there are concernswithmemory requirements.
- If the host system can't send raw IP packets at the same rate, a PGM implementation can't send athighrates.Thisnecessitatestheuseofappropriat eNICs,networkbuffersettings,andkernelsettings .Additionally, enough RAM to retain the whole transmission window may be required to assure high-speedfunctioning.
- Even at dialup data rates, network use for PGM is quite high, and even when SPMs are increased to 5persecond, network utilization remainsabove90%.
- SECURITY ISSUES: PGM is subject to a variety of security concerns, which are particular to thetechniqueitutilizestogeneraterepairstate,buildupsourcepathstate,recognizeDLRs,forwardNAKs,and disseminate repairs.
- Because network components switch as well as decrypt SPMs, NAKs, NCFs, and RDATA, all ofwhichmaybehonestlycommunicatedbyPGMsources,receivers,andDLRs,thesemethodsexposePGM network components to security threats. Short of full validation of every single receiver,adjoiningsource,networkcomponents,andDLRs,theprotocolisn'timpenetrabletomishandle.

EEvenwithoutaddressingPGM,theelementsrelated withDLRs,receivers,andsourcesaloneprovideenough security threats. These dangers include DOS due to CPU and memory exhaustion, as well asthelossof(repair) datacommunicationdue to the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 2 Feb 2022, pp: 1477-1482 www.ijaem.net ISSN: 2395-5252

obfuscationofrepair status.

- FalseRDATAmightcausePGMnetworkelementstodestroygenuinerepairstate,resultingintheloss ofactual RDATAinthe end.
- False NAKs may cause PGM network elements to enter a deceptive repair state that will end onlywhenthe timer expires, causingmemorydepletioninthemeanwhile.
- FalseSPMsmightcausePGMnetworkcomponentsto misdirectNAKsintendedforthe genuinesource,resultinginthe requiredRDATAnotarriving
- FalseNCFsmaycausePGMnetworkelementstoprematurelyceaseNAKtransmitting,resultinginthe lossofRDATA.

IV. SOMEPOSSIBLEEXSISTINGSOLUTIONS:

PGMisnotperfectandstillfacessecurityandotherissueswhichremainsforfuture workbutwe stillhave somesolutionsavailable that canbe used:

- ExtendingNAKsheddingtechniquestomanagebooththevolumeandthepaceofconfirmedNAKs.Regardless, these techniques aid network components in surviving NAK assaults at the expense ofservice availability. Network components might use the information on TSIs and their associatedtransmitwindowsacquiredfromSPMstoregulatethespreadofrepairstateevenmoreeffectively.
- Issues withbackchanneltrafficcanhandledusingFEC,FECalsohelpsinreducingprobabilityoflosingdata packets.
- FECcanhelpinnetworkutilizationas well, withoutFECeverypacket willbeneededtobesenttwice.
- In SPMs, jitter dampening of the network-header source address or path NLA value. While the networkheader source address is likely to change seldom, changes in fundamental multicast routing informationareexpectedtocause NLA'sroute tochange ona regularbasis.
- To prevent buffer invasion at the receiver, the receiver application should be aware of the handlingload necessary to read PGM packets from the network and give PGM a higher priority than otherapplication-leveltasks.
- Furthermore,operatingsystemsocketbuffersmustusuallybeenlargedtomeetthecapacitiesthatPGMtraffic froma well-tunedsender may reach.
- Athree-wayhandshakebetweennetworkelementsandDLRscanaidnetworkelementsindeterminingif a claimed DLR is PGM familiar and can be identified by the supposed network header sourceaddress.

V. CONCLUSION:

PGM is a material with a wide range of applications. It has a phased deployment method, with suppression inthe absence of router support and FEC managing a limited scaling load. As scalability requirements grow, PGMrouters can be given to add further scalability through hierarchy. The best scalability and performance may beattainedwhenallroutersactivatePGM.PGMutilizes apolling-basedNAKdelaytuningapproach.Thismethodworksfor bothscalingupanddown.

We also noticed that because to the utilization of FEC, NAK records, and unicast NAKs, PGM has a lot ofasymmetric aid. We've also demonstrated how PGM achieves high organization use despite sluggish (dialup)connections. PGM has proved that it can operate at high speeds (>100 Mbps). PGM is a new experimental RFCthat has been tested in both commercial and academic settings. Customer/server executions from Talarian(Smart PGM) and Microsoft are provided (Windows XP). PGM is now available on Cisco routers. Luigi Rizzohasgivenapublic source executionofPGM.

PGM isn't perfect, and it still has security flaws that must be resolved in the future, but there are a fewassurancesthatstand out,suchastheabilitytodampenchangesinthesenderaddressandPGMparentinSPMs(thesenderaddressshouldjustchangerarelyandthePGMparentshouldjustchangeonceinawhile,as the underlying multicast routing changes). NEs can defend themselves from sessions that create an excessivequantity of NAKs by leaving the session. A three-way handshake between NEs and DLRs would allow a NE tomore confidently verify whether a claimed DLR is PGM familiar and can be identified by the supposed networkheader source address.

VI. RELATEDWORKS:

Numerousothersolidmulticastanalystshaveexploredtheutilizationoforderedprogression,forinstance:

- Rizzo is responsible for the default erasure codes in PGM. Metzner was the first to suggest combiningFECanddependability.
- Suppression was pioneered by Ramakrishnan and Jain, and the SRM protocol pushed for reliablemulticast.
- Papadopoulos and Laliotis investigated the gradual deployment of LMS (a protocol that

shares manycharacteristicswithPGM)andfoundthateve npartialdeploymentincreasedscalabilityacrossr outers.Theybelieve that PGMwouldsee similar alterations.

- Bolotet.al.proposedpollingforfeedbackinamulti castsession.
- Rizzo also has presented a PGM-friendly TCP-friendly congestion management system. PGM NEs arenotrequiredtobe modified.
- Kermode'ssimulationsindicatehowcombiningF EC,suppression, and hierarchycanbebeneficial.
- Generic Router Assist (GRA) is a protocol that generalises several of the concepts in PGM such thattheyaren'tprotocolspecific.AswithPGM,atre eofGRA-capableNEsisconstructed asasubsetoftheIP multicast tree. GRA header fields that relate to "filters" are defined. Predetermined actions are takenwhen the header of a packet fits a filter definition. GRA filters, for example, might be used in PGM tohandleparityNAKsandparityretransmissions.
- PGMusesNAKlistsandFECwithsuppression, whichisidenticaltoNonnenmacheretal.

REFERENCES:

[1]. MARIA PSALTAKI, RODRIGO ARAUJO, GHADAH ALDABBAGH, PANAGIOTISKOUNIAKIS, ANDREAS GIANNOPOULOS, “Pragmatic General Multicast”, University collegeLondon.

[2]. Jim Gemmell, Todd Montgomery, Tony Speakman, NidhiBhaskar, Jon Crowcroft, “The PGMReliableMulticastProtocol”,University of Cambridge.

[3]. McClellanConsulting,"PragmaticGeneralMu lticast".

[4]. Dr. Jean-Claude Franchitti: “Main Theme IP Multicast”, New York Universityhttps://cs.nyu.edu/~jcf/classes/g22.2 262-001_sp10/slides/session10/IPMulticast.pdf

[5]. J. Crowcroft, J. Gemmell, D. Farinacci, S. Lin, D. Leshchiner, M. Luby, T. Montgomery, L. Rizzo, A.Tweedly,N.Bhaskar,R.Edmonstone,R.Su manasekera,L.Vicisano,“PGMReliabletransp ortprotocolspecification”.

[6]. N., Edmonstone, R., Sumanasekera, Speakman, T., Crowcroft, J., Gemmell, J. , Rizzo, L., Tweedly,Farinacci, D. , Lin, S., Leshchiner, D., Luby, M., Montgomery, T. , A., Bhaskar, R., Vicisano, L., PGMReliableTransportProtocolSpecification ,RFC3208

[7]. L. Rizzo, "pgmcc: A TCP-friendly Single-Rate Multicast Congestion Control Scheme", Proc. of ACMSIGCOMM.

[8]. C.Papadopoulos,"RAIMS:anArchitecture forRouter-AssistedInternetMulticastServices.”Zurich.

[9]. J.Chesterfield,A.Diana, A.Greenhalgh,M.Lad,andM.Lim,"ABSDRou terImplementationofPGM”

[10]. A.Giannopoulos,R.Araujo,G.Aldabbagh,P.K ouniakis,andM.Psaltaki,"PragmaticGeneral Multicast(PGM) hostimplementationfor FreeBSD."

[11]. http://web.jet.es/sola/inet98.html."Scalability ofInternetMulticastProtocols".

[12]. http://www.mcclellanconsulting.com/whitep apers/pgm.html.