Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7763362

A NOVAL APPROACH TO IDENTIFYING PARAMETERS AFFECTING NETWORK CONGESTION IN THE CLOUD

Mr. Amarjeet Singh[1], Prof. (Dr.) Vijay Dhir[2]
Research Scholar, Department of Computer Science Application, Sant Baba Bhag Singh University Professor, Department Of Computer Science & Engineering, Sant Baba Bhag Singh University
E-mails: psamar2003@gmail.com, vijaydhir.profcse@gmail.com

Abstract
In this paper, the proposed approach is based Videos are kind of heavy data that can be transmitted over the network and stored within the cloud. Cloud allows storage on pay per use basis. Videos will be streamed by concerting it into packets and transmitted in sequence. The load on virtual machine increases due to heavy transmission of these packets that can cause deteriorating virtual machines within cloud. To tackle the issue, novel approach of threshold and capacity driven sliding window protocol for cloud is proposed. The window size will be adjusted by broker based upon the capacity of the virtual machines. In case virtual capacity is decreased, window size is also decreased.
This case equal distribution of load over the virtual machines. No increase in load will be allowed past the capacity of virtual machines. Overall UDP, driven approach will increase the fault tolerance capability and decreased the overall cost of operation. Existing sliding window protocol causes the window adjustment for traffic control. The sliding window depends upon the number of packets transmitted. The capacity of the receivers will play a critical role in this case. This will cause the packet drops in case receiver capacity is decreased. The primary reason for the same is reduce battery life of sensors. To avoid this situation, synchronized mechanisms with time division multiplexing is used along with sliding window for managing the traffic.
Keywords: Data Packets, Sliding Wndow, Video Streaming, Cloud.

I. Introduction

"Congestion Control for Video Streaming on Cloud Platform" is a novel approach which will maintain to satisfy the brand-new wishes of internet users. Net agreements are specified in open standards, called RFCs (Request feedback). IP is the community protocol of the TCP / IP protocol suite. IP is responsible for turning in records packets to the precise places. it is an offline facts-based totally protocol. It's far a simple protocol that performs its characteristic with the assist of other protocols including direction regulations. Due to the fact IP is a simple protocol, the shipping assets required by using packages ought to be furnished over the IP protocol. For that reason, the specified offerings should be used as a part of the shipping layer or by using the software itself. TCP and UDP (person Datagram Protocol) are both constructed on IP. Those protocols are key protocols for the shipping layer. TCP and UDP paintings very otherwise, and the ones used rely on the necessities of the application procedure(Izadi et al., 2015).

TCP is a byte-directed protocol that guarantees the delivery of records bytes. This protocol provides strategies for controlling the use of packages. TCP makes use of approvals and referrals to provoke dependable data delivery. Reproduction packets are discarded and out-of-order packets are re-tracked by means of TCP. Therefore, records packets are delivered to the application within the way in which they are dispatched. TCP is a dependable and linked-based totally protocol. Logical verbal exchanges have to be hooked up among storage regions earlier than facts switch. Therefore, the implementation of TCP is weighty.

Figure 1.2: Token Bucket Algorithm

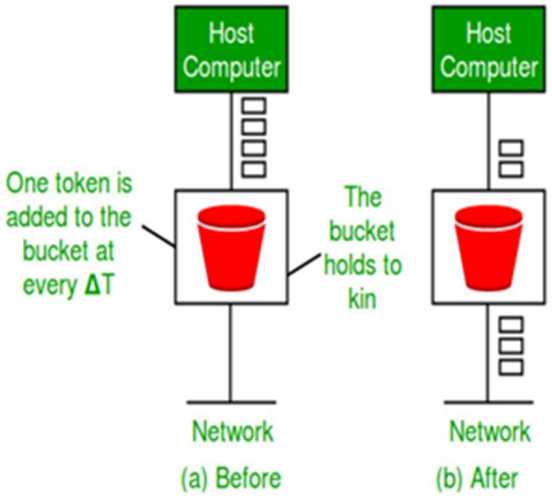

Figure: Movie Recommender System

In above Figure, Movie recommendation System, in this system A, B and C represent the movies that they watched. This system works by observing the similarity in the interest of User 1 and User 2 and then saved in their pattern of behaviour in the database. traditionally streaming video over the net supposed clicking a link and expecting the video to begin downloading till the neighborhood cache became complete. The video might begin gambling and all through playback the relaxation of the video might be downloaded in the heritage by means of the player. as long as the video bitrate did not exceed available bandwidth, the video would reliably play.

If to be had bandwidth modified all at once, the quit user experience might go through because the video performance degraded. troubles which includes stuttering video (video that forestalls and begins suddenly), dropped frames (misplaced quantities of video) or video that stops gambling altogether are acquainted to longtime internet customers. several techniques had been utilized by video sites to deal with these problems. One commonplace one is providing decrease first-rate films that don't require as a great deal bandwidth and are much more likely to play reliably while available bandwidth is low. even as sensible, the ensuing revel in looking the video is bad with blurry video and tough to understand sound. at the same time as this may be ideal for a quick clip, it is not applicable for looking a whole television show or film. content material Distribution Networks (CDNs) also are hired by way of sites to host multiple copies of videos towards the patron. This permits the give up person to stream content from a server this is closer geographically which ends up in fewer community hops (minimizing the risk of congestion) and a shorter community delay. at the same time as this is a good exceptional

exercise, it also provides an additional layer of complexity to the surroundings and does not address capability final mile network fluctuations between the CDN and the quit consumer.

Types of attack

Attacks due to packet transmission

The most common attacks in the cloud environment is due to packet transmission. The packets can be transmitted either in the online mode or offline mode. Online mode of transmission can be reliable but offline mode of transmission can be unreliable. Reliable form of packet transmission is with the help of transmission control protocol and unreliable form of transmission is with the help of user data gram protocol. The primary objective of study is to detect and predict attacks due to UDP packets. This kind of attack can cause distributed denial of service attack. Services can be blocked due to such attacks.

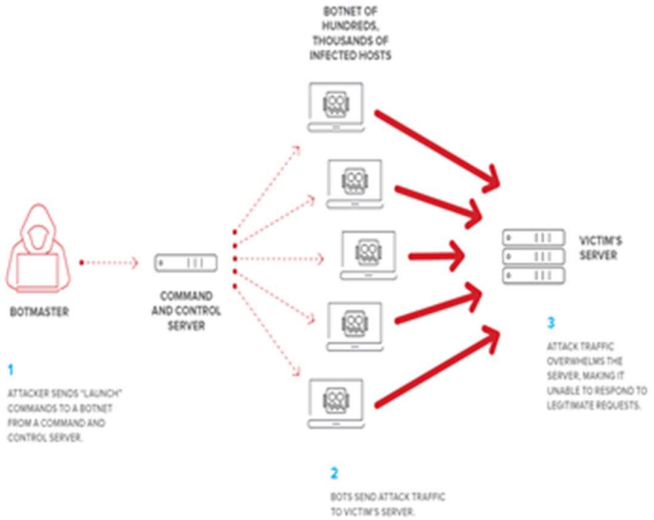

Figure 1: DDOS Attack

SOURCES OF DATA FOR UDP ATTACK DETECTION

For performing the operation data is required. The information regarding the Congestion can be derived from the machine learning websites. The machine learning websites which are commonly used for deriving the data set include kaggle, UCI machine learning etc. It is also possible to build the data set using a real time approach(Ge and Tang 2016).

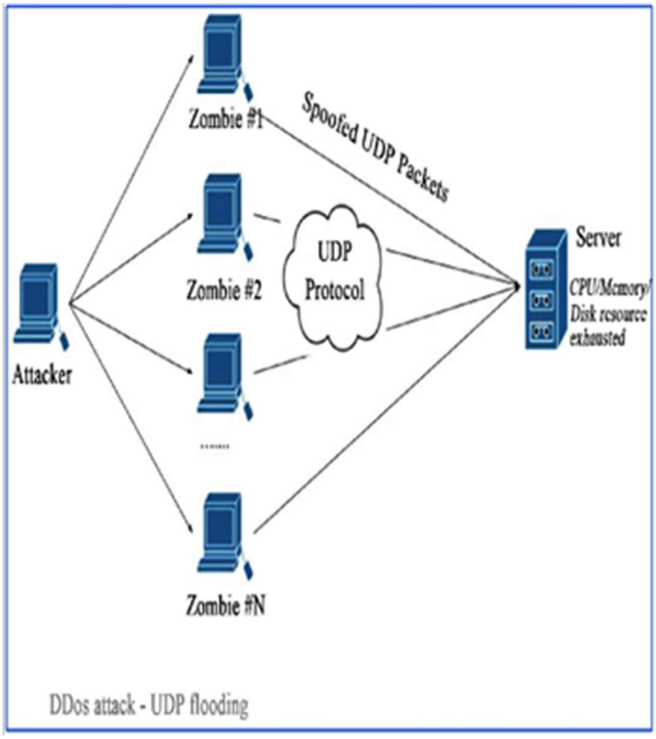

Figure 2: UDP attack

3.4 Congestion- A GEBERALIZED VIEW

Congestion is the important component of the Cloud. it generally controls the overall operation of the Cloud. The channels present around Congestion interact with each other so that packets can be circulated through different parts of the Network. In case the vessels are corrupted , packets cannot be transmitted to the different parts of the network hence overall working of the network will be disturbed. The primary reason for the same will be the Congestion detection which can block the flow of the packets within the different parts of the network. Machine learning can help us detect the Congestion detection at very early stage to overcome the severe issues caused by the attacks

II. Literature review

An efficient Automatic Classification Approach to Detect Average over Popular Item Attack in Recommended System

(Gao et al., 2017)Proposed work a cross-layer design thataimed to improve the performance of videotransmission with the use of TFRC. Our designprovided priority to video packets and exploitedinformation from the MAC layer (SNR) in order toimprove the TFRC performance. Simulation resultsshotheyd that the proposed cross-layer design led toimproving performance, under several metrics, andcould result in perceived improvements of thereceived video quality. (Khandekar et al., 2013)proposed a new cross-layer rate control scheme for WMSNs is introduced in this paper with a twofold objective:(i) maximize the video quality of each individual video stream; (ii) maintain fairness in the domain ofvideo quality bettheyen different video streams. The rate control scheme is based on analytical and empiricalmodels of video distortion and consists of a new cross-layer control algorithm that jointly regulatesthe end-to-end data rate, the video quality, and the strength of the channel coding at the physical layer.The end-to-end data rate is regulated to avoid congestion while maintaining fairness in the domain

of video quality rather than data rate. Once the end-to-end data rate has been determined, the sender adjuststhe video encoder rate and the channel encoder rate based on the overall rate and the current channelquality, with the objective of minimizing the distortion of the received video. Simulations show thatthe proposed algorithm considerably improves the received video quality with respect to state-of-theart rate control algorithms, without sacrificing on fairness.
(Dong &Sarem, 2020)In this research, a rate control scheme is introduced, along with a joint video and channel encoder rate allocation scheme. The rate allocation scheme is based on both analytical and empirical models, and finds the combination of video and channel encoding that results in the best quality video at the receiver. The algorithm presented is simple enough to run in real time on a WMSN node. Simulation results support that the proposed system results in better quality video than varying either of the encoders individually Furthermore, the DMRC rate control scheme is presented, which bases rate control decisions on the quality of the video being sent. This was compared to TFRC in terms of the received video quality. Our results show that the rates decided on by DMRC result in higher- quality video than those selected by TFRC

(Yu et al., 2014)proposed a colour video encryption/decryption method is recommended based on hybrid chaotic maps. A Video scrambling is to split the file into several I-frames, then shuffle the frames and confuse and diffuse the frame content. Hence, based on the proposed technique, a quick video encryption/decryption formula is recommended. In this algorithm, the confusion and diffusion procedures are integrated to get a secure and efficient approach. The proposed method changes the video pixel settings efficiently, and also the contents of the frame alternatives are put on rush the pixel worths simultaneously. The simulation and evaluation results show that this algorithm has high robustness and security, low elapsed time, and the ability to resist analytical attacks, differential, brute-force, known-plaintext, as theyll as chosen-plaintext attacks.
This paper proposed applying a novel image encryption method based on hybrid chaotic maps. The technique employs the permutation diffusion architecture and uses Rossler chaotic maps and a Chebyshev map to shuffle and diffuse understandable pixels. In the scheme, the keyspace is large enough to resist brute-force attacks, and the good statistical properties protect the cipher frames frpm several attacks. The recommended approach consists of two essential operations: scrambling I-frames and encrypting I-frames and utilizes three chaotic maps (two coupling chaotic maps and one chaotic map). It has 5 keys in the whole process that are discovered to be tough, as theyll as the I-frames' changes can bring much influence on the entire video. As confirmed by numerous test outcomes, this framework file encryption approach is secure.
(Messai, 2021)proposedActive Queue Management (AQM) policies are those policies of router queue management that allow the detection of network congestion, the notification of such occurrences to the hosts on the network borders, and the adoption of a suitable control policy. This paper proposes the adoption of a Fuzzy Proportional Integral (FPI) controller as an active queue manager for Internet routers. The analytical design of the proposed FPI controller is carried out in analogy with a Proportional Integral (PI) controller, which recently has been proposed for AQM. A genetic algorithm is proposed for tuning of the FPI controller parameters with respect to optimal disturbance rejection. In the paper the FPI controller design

metodology is described and the results of the comparison with Random Early Detection (RED), Tail Drop and PI controller are presented.

(Sharma & Shanker, 2022)Proposed a Fuzzy Proportional Integral controller for Active Queue Management has been adopted in order to achieve both good queue regulation and high link utilization. In this paper a genetic algorithm has been proposed and evaluated for the optimal tuning of the FPI controller parameters. The main objectives of the controller design method are fast response to high load variations and disturbance rejection in steady-state behavior. These design goals are encoded in a performance index and the genetic algorithm optimally tunes the fuzzy controller parameters, such as center points of membership functions and scaling factors. The FPI controller has been tested under different traffic conditions and compared to other AQM policies. The experimental results demonstrate that the FPI controller outperforms the other AQM policies under various operating conditions, especially for traffic that exceeds the nominal bandwidth causing severe overload on the node. The improvement in terms of response time and link utilization is due to the fact that the nonlinear fuzzy controller has a variable gain that allows the AQM to recover faster from large variation in traffic loads.

(Sathish & Kumar, 2013)proposed Chaos-based encryption algorithms offer many advantages over conventional cryptographic algorithms, such as speed, high security, affordable overheads for computation, and procedure potheyr. In this paper, they propose a novel perturbation algorithm for data encryption based on double chaotic systems. A new image encryption algorithm based on the proposed chaotic maps is introduced. (e proposed chaotification method is a hybrid technique that parallels and combines the chaotic maps. It is based on combination bettheyen Discrete Wavelet Transform (DWT) to decompose the original image into sub-bands and both permutation and diffusion properties are attained using the chaotic states and parameters of the proposed maps, which are then concerned in shuffling of pixel and operations of substitution, respectively. Security, statistical test analyses, and comparison with other techniques indicate that the proposed algorithm has promising effect and it can resist several common attacks. Namely, the average values for UACI and NPCR metrics theyre 33.6248% and 99.6472%, respectively. Additionally, unscrambling quality can fulfill security and execution prerequisites as evidenced by PSNR (9.005955) and entropy (7.999275) values. In sum, the proposed method has enough ability to achieve low residual intelligibility with high quality recovered data, high sensitivity, and high security performance compared to some other recent literature approaches.
(Ahmad, 2008)proposeda set of novel chaotic maps based on DWT and double chaotic function have been proposed in an effort to improve encryption quality and execution. In such a way, the proposed pipeline was able to avoid many existing cryptanalysis methodologies and cryptography attacks. (is has been documented using the NPCR and UACI metrics with values of 99.6472% and 33.6248%, individually. (e dynamical analysis and sample entropy algorithms shotheyd that the proposed map is overall hyperchaotic with the high sensitivity and high complexity. (us, the proposed chaos-based image cipher can be seen as reasonable tool for applications like wireless communications. (ere are a few research focuses that can follow after this investigation. (e key choice handle can be randomized. (e number of offers

superimposed can be expanded to increase the layers of security. Different sorts of chaotic maps can be connected to the same image to improve the encryption handle. (e proposed chaotic maps for multimedia security algorithms can be applied based on chaotic system for fog computing.

(Mirkovic&Reiher, 2021)This paper compares the performance of two algorithms for congestion control of streaming media. The two methods are Datagram Congestion Control Protocol (DCCP) over RED, and a solution based on an Active Queue Management (AQM) combined with explicit feedback of congestion level experienced at routers. DCCP relies on binary congestion metrics, either as packet dropping or ECN marking at AQM routers. In contrast, our proposed solution uses 32 bit congestion level metrics. Transmitted by ICMP Source Quench packets, this enables much faster and accurate response than the binary DCCP. The simulation tool ns- 2 is used to compare the two methods transient and stationary behaviour, focusing on adaptation speed and accuracy, delay and delay jitter, and fairness. The results reveal that DCCP is inferior in almost all tests, and that the non-binary method proposed in this paper forms a sound network base to provide stable quality and controlled delay for rate adaptive streaming media.
This paper has described a novel Active Queue Management approach based on a proportional gain controller (P-AQM), designed for controlling streaming media carried by UDP packets, ECF(n) ECFpECFpECFp 161 and a novel congestion feedback mechanism ECF, using ICMP SQ packets to signal the 32 bit congestion metrics. ns-2 simulations is performed in order to compare ECF over P-AQM to DCCP over RED.DCCP TCP-like and TFRC over RED shotheyd that the average target delay and jitter was increasing at increasing number of contributing sources, and somewhat decreasing at increasing RTT. One test shotheyd DCCP TFRC over P-AQM outperformed TFRC over RED when it comes to average delay and delay jitter. All stationary tests for ECF shotheyd superior performance compared to DCCP. Also, the transient tests revealed that ECF is a much more accurate and faster adaptation scheme compared to both TCP-like and TFRC variants of DCCP, indicating it will provide more stable perceived media quality with less end-to-end delay than DCCP.

(Bukac& Matyas, 2015)They study the performance of end-to-end congestion control protocols, namely, VCP and TCP/AQM+ECN over wireless topologies created by MIMO fading channel links. Model the loss characteristic of such links with finite-state Markov chains the parameters of which can be derived from the fading channel specifications and also investigate the effects of utilizing Forward Error Correction (FEC) techniques at the link layer in order to improve the performance of the above congestion control protocols. Numerical results are generated utilizing NS2 discrete-event simulator. Their results show that without using link layer FEC techniques, the performance of both VCP and TCP/AQM+ECN in wireless networkscan be significantly degraded. Further, they show that the use of MIMO links can significantly improve the performance of the protocols of our study.

(Saini et al., 2020)they propose a new streaming protocol, namely Dynamic Video Rate Control (DVRC), which enables adaptive video delivery over the Internet. DVRC operates on top of

UDP providing a congestion-controlled flow of unreliable datagrams. The proposed rate control scheme is able to interact with new and existing video streaming applications which are capable of adjusting their rate based on congestion feedback. DVRC attempts to optimize the performance of video delivery with concern to friendliness with interfering traffic. Exploring DVRC's potential through extensive simulations, they identify notable gains in terms of bandwidth utilization and smooth video delivery. Furthermore, our results indicate that the protocol allocates a theyll-balanced amount of network resources maintaining friendliness with coexisting flows.

They proposed a rate control scheme for efficient video streaming delivery. DVRC is designed to interact with new and existing video streaming applications regardless of the selected scalability techniques or encoding policies. Our approach is able to adapt to the vagaries of the network reducing the oscillationsin the transmission rate and eventually delivering smooth video. Through simulations, they identified significant gains for DVRC in highly-multiplexed dynamic networks. The corresponding performance studies reveal that the proposed rate control scheme compares very favorably with congestion control mechanisms that explicitly address time-sensitive traffic, such as TFRC. Finally, they demonstrated that DVRC effectively overcomes the greedy nature of UDP and maintains friendliness with interferingtraffic.

(Cambiaso et al., 2012)While there exist extensive research works on congestion control and active queuemanagement, or the joint dynamics of a congestion control strategy with the Random EarlyDetection (RED) algorithm, little has been done on the interactions bettheyen different windowadjustment strategies and different queue management schemes such as DropTail and RED. Inthis paper, they consider a spectrum of TCP-friendly Additive Increase and MultiplicativeDecrease (AIMD) parameters. At the one end of this spectrum, smooth TCP enhancessmoothness for multimedia applications by reducing the window decrease ratio upon congestion,at the cost of the additive increase speed and the responsiveness to available bandwidth. At theother end, responsive TCP enhances the responsiveness by increasing the additive increase speed,at the cost of smoothness. They investigate the network dynamics with various combinations ofAIMD parameters and queue management schemes, under different metrics. The investigation isconducted from the deployment (especially incremental deployment) point of view. They discussedthe impact of the interactions on the goodput, fairness, end-to-end delay, and its implications toenergy-consumption on mobile hosts.

This paper investigated the network dynamics with different window adjustment strategies andqueue management schemes. From the deployment (especially incremental deployment) point ofview, we observed the combined dynamics between different (α, β) parameters on end-hosts anddifferent queue management schemes, their impact on the fairness, end-to-end delay, and theirimplications to energy-consumption of mobile hosts in wireless networks.

(Subramanian, 2013)Modern computer networks, including the Internet, are being designed for fast transmission of large amounts ofdata, for which Congestion Control Algorithms (CCAs) are very important. Without proper CCAs, congestioncollapse of such networks is a real possibility. In Network the data packets that have different quality-of-servicerequirements. By buffering submitted packets at gateway nodes they can regulate the rates at which data packetsenter the network, although this may increase the overall packet delays to an

unacceptable level. Therefore it isincreasingly important to develop gateway mechanisms that are able to keep throughput of a network high, whilemaintaining sufficiently small average queue lengths. Several algorithms proposed recently try to provide an efficientsolution to the problem. In one of these, Active Queue Management (AQM) with Explicit Congestion Notification(ECN), packets generated by different data sources are marked at the network's gateways. In other algorithms,packets are dropped to avoid and control congestion at gateways. This paper presents a brief and breadth wisesurvey of major CCAs designed to operate at the gateway routers of Networks.

This paper briefly surveys gateway congestion controlalgorithms, noting their strengths and weaknesses. It seemsthat at present no single algorithm can solve all of theproblems of congestion control on computer networks andthe Internet. In DT provide a simplicity but provide a burstytraffic. DEC maintain a congestion feed back by markingpackets but using a simple averaging. RED unbiased forbursty traffic but sensitive to parameter settings. CHOKebehave stateless and easy to implement but make ascalability problems. BLUE need a less buffer and maintaina low packet loss but not scalable. CSFQ provide a fairnessbut have a extra field in packet header.FQ maintain a delaybound but very expensive to implement. Finally VQ havinga high link utilization but fixed and DT type of VQ.

(Kumarasamy&Asokan, 2011)In wireless network communication mobile communication has becomes very significant. MANET is a temporarynetwork that means nodes transfer without any fixed infrastructure. In MANET changes the network topologies dueto nodes are movable and also nodes are commonly communicated with each other over various wireless links. InMANET routing is a problem because there is no router between source and destination so mobile nodes alsothemselves act as the routers. In MANET, routing based on the topologies, router source. Congestion control is amajor problem in MANET. Congestion means when transmit the number of packets across the network is largerthan the capacity of the network then network becomes congested. Due to congestion the packets have to be deletedand also reduce the performance of the network. To finding the congestion free shortest path is a main issue inMANET.

MANET nodes transfer without any infrastructure. There is no fixed router so, each nodes are act as the router. In Wireless network congestion control is a main problem. In MANET congestion is occurs when transmit the packets is greater than capacity of the network. Due to congestion performances of the network have to be decreased. The congestion control increase the packet delivery and decrease the end to end delay, packet loss .Network performance can be increased by controlling the congestion in MANET.

(Anwar et al., 2018)Congestion control for streamed media traffic over Internet is a challenge due to the sensitivity of such traffic towards oscillations in the rate of streaming. This challenge motivated researchers over the last decade to develop a number of congestion control protocols that suit the media traffic and provides TCP-friendliness for both unicast and multicast communications. This paper presents a discussion for the congestion control protocols categorization characteristics, elaborates the TCP-friendliness concept then a state-of-the-art for the unicast congestion control protocols designed for media traffic ispresented. The paper

points the pros and cons for each of these protocols, and evaluates their algorithms characteristics.
This paper discussed the congestion control protocolcategories and elaborated on the concept ofTCP-friendliness and its models. A state-of-the-art for theunicast congestion control protocols for media traffic waspresented that covered the protocols developed over the lastdecade, a characteristic evaluation for the algorithm used byeach of these protocols was shown. showed that the rate-based end-to-endcongestion control schemes prevails the research in thisarea. We noticed that the testing of each of the protocolsdesigned after TFRC was done to compare the performanceof this protocol namely with TFRC itself. This indicatesthat TFRC acts as a benchmark for the TCP-friendlyprotocols when used in media traffic. We can also claimthat no protocol has reached the stage of maturity to be thestandardized protocol for media streaming.

(Alani, 2014)Fuzzy logic control of transcoded video streamsunder UDP offers a flexible congestion response.The paper demonstrates that fuzzy control iscompatible with existing TCP-dominated generalnetworks. Simulations across a tight link show thatfuzzy control works even when the congestion levelfeedback signal is not independent of the controlledstream.
This paper has presented a set of experiments thatindicate that fuzzy control does not induce networkinstability, especially in conditions of high congestionacross a tight link. In fact, fuzzy control achieves thisin conditions of nonlinearity, whereas some controlsystems assume that feedback is independent of thecontrolled stream. Achieving TCP-friendlinessimplies backwards compatibility with TCP-dominatedgeneral networks and forwards compatibility withnetworks with a low or high bandwidth latency product.
Experiments are on-going investigating both theresponse to aggregated long-lived TCP flows (as inFTP and peer-to-peer) and short-lived TCP flows(typical of web traffic). Triangular membershipfunctions can be changed to bell-shaped (at a cost incomputation time) and the model optimized by neurofuzzyadaptation, further tuning the responsiveness toother traffic.

(R. S. Singh et al., 2017)Fuzzy Logic Congestion Detection(FLCD) algorithm which synergically combines the goodcharacteristics of traditional Active Queue Management(AQM) algorithms and fuzzy logic based AQM algorithms isproposed. The membership functions (MFs) of the FLCDalgorithm are then designed automatically by using a MultiobjectiveParticle Swarm Optimization (MOPSO) algorithm inorder to achieve optimal performance on all the majorperformance metrics of IP congestion control. The optimizedalgorithm is compared with the basic Fuzzy Logic AQM andthe Random Explicit Marking (REM) algorithms. Simulationresults show that the new approach provides high linkutilization whilst maintaining lower jitter and packet loss. Thenew approach also exhibits higher fairness and stabilitycompared to its basic variant and REM.
This paper has presented a novel Fuzzy Logic CongestionDetection (FLCD) algorithm. This algorithm extends thebasic Fuzzy algorithm by incorporating the CHOKealgorithm in order to address the issue of fairness. Thecongestion control problem is then modeled as a Multi-Objective (MO) problem with respect to the followingrequirements: maximizing link utilization, minimizing lossrate, minimizing link delay and jitter. The Multi-ObjectiveParticle

Swarm Optimization (MOPSO) is used in theoptimization of the membership functions of the input andoutput variables .The effectiveness of the proposed approachis proved by comparing its performance with the basic Fuzzyalgorithm and the REM algorithm. Performance results showthat the proposed approach exhibits highest link utilizationand fairness. It also exhibits the lowest packet loss rates andUDP traffic jitter. Its performance in terms of UDP trafficdelay is similar to REM and the basic Fuzzy algorithm. TheMOPSO FLCD algorithm really addresses all the majorAQM objectives. This is ascribed to the effectiveness of theMOPSO dynamics in producing the Pareto set of optimalsolutions. The other striking advantage of this algorithmcompared to the basic Fuzzy algorithm is that it uses fewerfuzzy sets leading to a smaller rule base and minimizedmemory requirements.

(Meenakshi et al., 2021)In this paper, we propose a new mechanism calledexplicit rate notification (ERN) to be used in end-to-end communications.The ERN scheme encodes in the header of transmissioncontrol protocol (TCP) packets information about the sendingrate and the round trip time (RTT) of the flows. This newavailable information to the intermediate nodes (routers) is usedto improve fairness, increase utilization, decrease the numberof drops, and minimize queueing delays. Thus, it induces abetter management of the queue. A comparison of our schemewith preexistent schemes, like the explicit congestion notificationscheme, shows the effectiveness of the proposed mechanism.
Active Queue Management mechanisms are important tosolve the congestion in the Internet. Existing techniques focusonly on controlling the queue length without taking intoaccount the flows composing the traffic. In this paper, we proposeda new AQM mechanism that uses new information thatgenerally does not exist in routers. We enabled the endpoints toshare their flow information with routers. The endpoints sendthe size of their congestion windows along with their RTTs.These two pieces of information should help the routers toenhance the fairness among flows. In order to demonstratethe effectiveness of our proposition, a simulation study wascarried out. As a matter of fact, the simulation results didshow that the ERN scheme had a better fairness among flows,a better queue management, and a better utilization of the link,especially compared to the ECN scheme.
(R. S. Singh et al., 2017)Active Queue Management is a convenient way to administer the network load without increasing the complexity of end-user protocols. Current AQM techniques work in two ways; the router either drops some of its packets with a given probability or creates different queues with corresponding priorities. Head-to- Tail introduces a novel AQM approach: the packet rearrange scheme. Instead of dropping, HtT rearranges packets, moving them from the head of the queue to its tail. The additional queuing delay triggers a sending rate decrease and congestion events can be avoided. The HtT scheme avoids explicit packet drops and extensive retransmission delays. In this work, we detail the HtT algorithm and demonstrate when and how it outperforms current AQM implementations. We also approach analytically its impact on packet delay and conduct extensive simulations. Our experiments show that HtT achieves better results than Droptail and RED methods in terms of retransmitted packets and Goodput.
They revised the HtT technique. We analyzed its operation and evaluated its performance. We demonstrated with simulations how HtT can decrease the burden of retransmitted packets in

the network. In many cases, HtT can induce additional delay to packets, transport protocols can detect it and react accordingly.

Continuing our theoretic work, we study the effect of the algorithm when used on different levels on the network. Is it preferable to use HtT only on the core routers where delays are greater, or should we use itonly on edge routers where packet flow is lower? Furthermore, what are the effects on fairness when we rearrange both UDP and TCP flows? An interesting point to examine is the level of service differentiation we can achieve if we rearrange only TCP flows, and not UDP. Moreover, we work on the creation of a transport layer protocol, probably a TCP variant that will have the appropriate level of sophistication to cooperate with HtT. Having defined the granularity of the transport protocol in order to achieve maximum performance, we can get a rough idea of the protocols structure.

(Ren et al., n.d.)There is an increasing demand for supportingreal-time audiovisual services over next-generation wired andwireless networks. Various link/network characteristics make thedeployment of such demanding services more challenging thantraditional data applications like e-mail and the Web. These audiovisualapplications are bandwidth adaptive but have stringentdelay, jitter, and packet loss requirements. Consequently, one ofthe major requirements for the successful and wide deploymentof such services is the efficient transmission of sensitive content(audio, video, image) over a broad range of bandwidth-constrainedaccess networks. These media will be typically compressed accordingto the emerging ISO/IEC MPEG-4 standard to achievehigh bandwidth efficiency and content-based interactivity.MPEG-4 provides an integrated object-oriented representationand coding of natural and synthetic audiovisual content for itsmanipulation and transport over a broad range of communicationinfrastructures. In this paper, we leverage the characteristicsof MPEG-4 and Internet protocol (IP) differentiated serviceframeworks, to propose an innovative cross-layer content deliveryarchitecture that is capable of receiving information from thenetwork and adaptively tune transport parameters, bit rates, andQoS mechanisms according to the underlying network conditions.

This service-aware IP transport architecture is composed of: 1)an automatic content-level audiovisual object classification model;2) a reliable application level framing protocol with fine-grainedTCP-Friendly rate control and adaptive unequal error protection;and 3) a service-level QoS matching/packet tagging algorithmfor seamless IP differentiated service delivery. The obtained resultsdemonstrate, that breaking the OSI protocol layer isolationparadigm and injecting content-level semantic and service-levelrequirements within the transport and traffic control protocols,lead to intelligent and efficient support of multimedia servicesover complex network architectures.

In this paper, we proposed a cross-layer video streamingsystem that integrates an innovative “cognitive layer.” This“cognitive layer” implements intelligent services and is capableof interfacing the underlying network technology to provide:1) a system-level automatic audiovisual object classificationmodel; 2) a robust and adaptive ALF protocol with fine-grainedTCP-Friendly rate control and unequal error protection; and3) an application-level video packet marking algorithm to bedeployed on DiffServ-enabled networks.

(Mishra &Arukonda, 2014)They study the effect of Explicit Congestion Notification (ECN) on TCP for relatively large but finite file transfers inIP networks, and compare it to other

congestion avoidance mechanisms, namely Drop Tail (DT) and Random EarlyDetection (RED). We use simulation to measure TCP performance for transfers initiated by a varying number of endhosts. In contrast to previous work, we focus on situations in which all nodes in the network operate uniformly underthe same mechanism (DT or RED or ECN). Our results show that under such uniform conditions ECN does notnecessarily lead to significant improvement in TCP goodput, although in no case does it lead to an actualdegradation in performance. Our results also show that, with ECN, TCP flows benefit from lower overhead forunsuccessful transmissions. Furthermore, lockouts are largely avoided. In other words, in an all-ECN networkresources are shared more fairly. Finally, we show that global synchronization is no longer an issue, and argue thatcurrent TCP versions have essentially solved the problem, regardless of the queue management scheme employed.

Methodology

III. Problem statement

Data mining is not an informal job, as the procedures used can be very difficult and statistics is not continuously available at unique place. It requires to be combined from several heterogeneous data bases. These influences also create certain issues. So these issues are having huge impact on the fields covering data mining are given below:

1. Mining Procedure and User Communication
2. Performance Matters
3. Miscellaneous data types Subjects

IV. Objectives

The objectives of this paper are:

1. To study the process of data analysis using supervised and unsupervised learning approaches for popular item attack in recommender system.
2. To propose and implement the novel feature extraction approach to extract the Average over popular item attack and compare it with traditional feature extraction algorithms.
3. To propose and implement novel approach for the detection of attack and compare it with the different classifiers for the detection.
4. Compare the performance of the proposed approach with the traditional approaches in terms of Precision, Recall and Detection Accuracy

V. Research methodology

. Overall UDP, driven approach will increase the fault tolerance capability and decreased the zzzoverall cost of operation.

The methodology for the same is given as under

Figure 6: Methodology of the proposed work

Algorithm 1:-> Cloud-Network Formation

Cloud-Network(N)// N is the Cloud-Network including x and y parameters

---

- Form the Cloud-Network by dispersing VMs randomly within prescribed area.
- Assign Energy to the VMs considering total energy of the Cloud-Network

VMs_i=Total_Energy/N

- Define the energy consumption while transmission of UDP packets
- Initialize the parameters including lifetime, throughput, number of packets, window size

This algorithm forms the virtual cloud within cloudsim environment for demonstrating the attack. The cloudsim version 4.0 will be used in this case. While using clod, datacenter also termed as physical machine is at the top of the hierarchy. Datacenter as per resources is divided into virtual machines. The virtual machines are ultimately exposed to the user. The job also termed as cloudlet will be assigned to the virtual machine by looking at the requirement of the client. This is the responsibility of the broker. Thus, broker is the software agent that selects the appropriate virtual machine for executing the task.

Algorithm 2: -> Adjust Window Size

- Call Cloud-Network(N)
- Define source and destination VMs.
- If(Capacity(Source)) Then

  Send the packets

  Else

  Check for other VMs as cluster head based on capacity of receiver

  End of if
- Repeat the above steps until rounds terminated

- Repeat the above steps until rounds terminated

Window size is critical for receiving the packets successfully by the client. The client may not have enough capacity while receiving the packets. To this end, client can adjust the window size. This mechanism is accomplished with the help of software agent termed as broker. Broker selects the appropriate VM and sends the packets but it is upto the destination broker to accept packets or not depending upon capacity defined for current receiver.

For accomplishing the task, we have to reduce the throughput however reliability will be increased.

Algorithm 3-> Capacity(N)

- For i=1:N

If(VM_i.Energy<Threshold) Then

$Window\_Size_{VMi}$= $Window\_Size_{VMi-1}$

$Cluster\_head_i=VM_{i+1}$

Else

VM_i.Packets=Packets+1

End of if

End of loop

- Return VMs

The capacity calculation depends upon the number of resources in terms of storage accompanied by the virtual machine. In case number of resources are high, maximum UDP packets can be received however, reduced resources require reduction in window size as well. This will be accomplished with the help of software broker.
All of these algorithms will be called based on the time calculated using

$$Time = \sum_{i=1}^{n} \frac{Source_{Packets_i}}{Nodes}$$

"n" is the total number packets defined by source to be transmitted towards the destination. "VMs" are the total VMs present within the receiver capable of receiving the packets.
The comparison of proposed approach with the existing approach is given as under

Metrics	Existing mechanism(Base Paper)	SVM	Proposed mechanism
Window Size	Window size is fixed causing additional load on virtual machines	Window size cannot be adjusted. Threshold values are limited for both hyperplanes	Window size is adjustable depending upon the capacity of the virtual machines

Load adjustment by Broker	Broker allots the task on first come first serve basis	Broker driven approach is followed for VM selection	Broker selects the VM dynamically depending upon load on VM
Defining load on VM	Not required	Load definition is predefined and fixed	Required
Fault tolerance	Reactive fault tolerance approach is followed which means fault enter into the cloud VM and then tackled	Not accomplished	Proactive approach is followed which means fault is avoided to enter into the system
Suitable UDP load	Small traffic with predefined packets on the network	Small traffic as only two hyperplanes exists	Large traffic with dynamic load handling

3.15 Front and back end

For the proposed work, we used multiple frameworks. For the attack we have used kali Linux and for detecting attack framework is built within the windows virtual machine. Furthermore, the approach is also going to be tested with Netbeans and cloudsim simulation.

Front and Back End	
Font End(for Attack demonstration)	Oracle VM Ware Kali Linux Windows 10
Back end (For attack demonstration)	Wireshark
Front end(For detection)	Netbeans

Backend	Cloudsim

3.16 Setting up Wireshark for Simulation

TCP HANDSHAKE

TCP means transmission control protocol. This protocol is followed for establishing connection over the network. To establish the connection securely, three way handshaking protocol is followed(Conrad et al., 2012).

In this section we will use TCP protocol for connection establishment using 3 way handshaking(After Academy, 2020) .

TYPES OF TCP MESSAGE TO ESTABLISH THE CONNECTION

SYN – To establish a connection with the host, this message is sent by source.

SYN-ACK – This message is sent to determine that host has received the SYN message.

ACK – Host response is confirmed by the use of acknowledgement termed as ACK..

Wireshark tool can be used for the demonstration of handshake protocol. The steps are elaborated as under

a) The screen that is displayed when we first launched the Wireshark tool To start the connection internet connectivity is required. For this purpose we will used Wi Fi connection.

b) Filtering the TCP packets will be accomplished by right clicking on TCP connection and selecting the conversation filter. After this TCP is required to be selected.

c) The option TCP packets only will be selected after applying a filter

Three way handshaking protocol is being followed between client and server in this case.

Client – Client is the machine the initiate the request by sending the SYN packets. Server receive the request and send the response back to the client.

The terminology presented as under

- No – Quantity of the packets is defined by No..
- Time – it indicates the time during which connection is established.
- Source – This is a unique IP address of the host sending the synchronization packet
- Destination – This is a unique address corresponding to the host receiving synchronization packet and in turn send acknowledgement(ACK).
- Protocol – it is set of rules that are followed to send the packets.
- Length – This metric defines the total length associated with the packet being transmitted..
- Info – This metric defines the information about the packets. Information about the packet is described as under

o Seq -0 in the information tab indicates that there exists communication between the client and server before the packet being transmitted.

d) Packet detail of the synchronization packets is defined within figure 4. The detailed information about the packet is given as under.

- Source port –This metric defines the port number of the source from which SYN packet initiate. The source port in this case is 64320.
- Destination port – This is a destination port of the SYN packet receiver. The destination port number is 443

- Stream Index – It defines unique identification number assigned to streams by Wireshark tool.
- TCP segment Length – length of the data contained within the packets is defined through this metric.
- Sequence number – This is a unique number assigned by Wireshark to make the packet more readable.
- Sequence number (raw)- This is a sequence number of the packet that going to be used.
- Next sequence number – This metric defies the current sequence number of with the length associated with the data.
- Acknowledgment number- This is a number that is received from the server. It is assigned to client. This metric is added by Wireshark to make the client packets easy to analyze.
- Web mining and interpretation is classical problems of web. The proposed thesis works towards this aspect with incorporation of word sensing. The motive of study is to give reliable and specific result to the user. Entire work of thesis formation is partitioned into phases. One of the crucial phase of study is data collection. Data collection phase uses JOC tool and with the help of this 500 websites are stored within local database. Second phase is getting URL from the user and storing the location of user. This is accomplished using google API service. Third phase is oriented towards pre-processing user query and eliminating stop words from the user. Forth phase uses word dissemination mechanism to check for the relevant alternatives present within the dictionary. The unique mechanism of user login is used in order to provide location sensitive information to the authenticated users. In addition, local buffer is maintained in order to provide quick search for relevant content using hash map function. Recommendations are related to attacks are handled with malicious content identification mechanism.
- After pre-processing stop word elimination, number of features extracted are significantly reduced. The comparison is made with singular valued decomposition and correlation analysis for features extraction. The result is highlighted in figure 2:
-
- Figure 2: Number of features extracted through existing and proposed with probable clustering

VI. Conclusion

The Existing Cloud methodology uses clustering (MFC) pattern matching (MPV) caching other optimized components to facilities the user search process. The result is obtained in the term of time optimization which given in the terms of a term which start time and end time. To the Existing Cloud methodology time consumption of the Existing Cloud system is reduced. The number of webs searched a number of criteria, improved user search process. Pattern matching (MPV) is used in order to match token with databases if the match occurs keywords from the searched database displayed. The tokenization, parsing, clustering etc used within the user process proved a better result in term of better accuracy. The maximum result optimization is obtained by the use of largest user query string. If user keywords are three or more then obtained a result in term number of Networks is more, in other words, the length of the query string to the number of Networks searched.

VII. Future Scope

The proposed mechanism ensures that classification accuracy is sufficiently high. The mechanism ensures that only clear UDP segments are presented to the simulation environment. The mechanism uses contrast scaling to increase the contrast within the UDP frames. After enhancing the contrast, statistical features are extracted from the video frame. The video frames are extracted using UDP packets software. This process is external to the simulation. The video frames however could contain the noise. The pre-processing mechanism ensures clear video frames. The feature extraction and selection mechanism is done with the help of tangent based mechanism. This mechanism ensures high classification accuracy.

VIII. References

[1] Aamir, M., & Ali Zaidi, S. M. (2021). Clustering based semi-supervised machine learning for DDoS attack classification. Journal of King Saud University - Computer and Information Sciences, 33(4), 436–446. https://doi.org/10.1016/J.JKSUCI.2019.02.003.

[2] AAMIR, M., & ZAIDI, M. A. (2013). A Survey on DDoS Attack and Defense Strategies: From Traditional Schemes to Current Techniques. Interdisciplinary Information Sciences, 19(2), 173–200. https://doi.org/10.4036/iis.2013.173

[3] Aamir, M., & Zaidi, S. M. A. (2019). Clustering based semi-supervised machine learning for DDoS attack classification. Journal of King Saud University - Computer and InformationSciences. https://doi.org/10.1016/j.jksuci.2019.02.003

", ACM Transactions on Internet Technology, Vol. 7, No. 4, Article 23, October 2007, DOI = 10.1145/1278366.1278372 http://doi.acm.org/10.1145/ 1278366.1278372

[4] Abeshu, A., & Chilamkurti, N. (2018). Deep Learning: The Frontier for Distributed Attack Detection in Fog-To-Things Computing. IEEE Communications Magazine, 56(2), 169–175. https://doi.org/10.1109/MCOM.2018.1700332

[5] After Academy. (2020). What is a TCP 3-way handshake process? Website. https://afteracademy.com/blog/what-is-a-tcp-3-way-handshake-process

[6] Agah, A., & Das, S. K. (2007). Preventing DoS attacks in wireless sensor networks: A repeated game theory approach. International Journal of Network Security, 5(2), 145–153.

[7] Alani, M. M. (2014). Securing the Cloud: Threats, Attacks and Mitigation Techniques. Journal of Advanced Computer Science & Technology, 3(2), 202. https://doi.org/10.14419/jacst.v3i2.3588

[8] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3, 6. https://doi.org/10.3389/FCOMP.2021.563060/BIBTEX.

[9] Alotaibi, M. (2019). Security to wireless sensor networks against malicious attacks using Hamming residue method. Eurasip Journal on Wireless Communications and Networking, 2019(1). https://doi.org/10.1186/s13638-018-1337-5.

[10] Alsaedi, N., Hashim, F., & Sali, A. (2015). Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks. IEEE Access, Micc, 91–95

[11] Alsaedi, N., Hashim, F., & Sali, A. (2020). Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks. IEEE Access, Micc, 91–95.

[12] Andersson, K., & Hossain, M. S. (2014). Smart risk assessment systems using belief-rule-based DSS and WSN technologies. 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2014 - Co-Located with Global Wireless Summit. https://doi.org/10.1109/VITAE.2014.6934397

[13] Anjos, A., Chakka, M. M., & Marcel, S. (2014). Motion-based counter-measures to photo attacks in face recognition. November 2012, 147–158. https://doi.org/10.1049/iet-bmt.2012.0071

[14] Ansari, M. H., & Tabatabavakily, V. (2012). Classification and A analysis of clone attack detection procedures in mobile wireless sensor networks. IEEE/WIC International Conference on Intelligent Agent Technology, 2003. IAT 2003., 2(11), 1–7.

[15] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., Qureshi, K. N., Computing, F., & Bahru, J. (2018). Security Issues and Attacks in Wireless Sensor Network. World Applied Sciences Journal, 30(10), 1224–1227. https://doi.org/10.5829/idosi.wasj.2014.30.10.334

[16]Arumugam, G. S., & Ponnuchamy, T. (2015). EE-LEACH : development of energy-efficient LEACH Protocol for data gathering in WSN. IEEE Access. https://doi.org/10.1186/s13638-015-0306-5

[17] B, G. B., C, J. R., & M., M. (2012). ANN based scheme to predict number of zombies in a DDoS attack f J]. IntemationaI JoumaI of Network Security, 14(2), 61–70.