Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.279 – 284

RESEARCH ARTICLE

SERVER TRAFFIC CONTROLLER DURING VIDEO STREAMING

J.Lakshmi, Mrs. S.Vijayalakshmi, M.E

B.E –CSE, Associate Professor (CSE)

IFET College of Engineering, Villupuram

Lakshmijayaraman19@gmail.com

ABSTRACT

Traffic balancing in the wireless network environment has an important impact on the performance. Multimedia streaming applications and services, trusted video delivery to prevent undesirable content-leakage has, indeed, become critical. Their detection performance substantially degrades owing to the significant variation of video lengths. We focus on overcoming this issue by proposing a round robin algorithm and best-partition searching algorithm that is robust to the variation of the video length. We enhance the detection performance of the proposed scheme even in an environment subjected to variation in length of video. Through a test experiment, the effectiveness of our proposed scheme is evaluated in terms of calculate the length of video, delay variation, and packet loss.

Good Traffic balancing makes wireless network more efficient and improves user satisfaction. This article introduces a better traffic balance model for the public Network based on the Networking concept with a switch mechanism to choose different strategies. The algorithm applies the game theory to the Traffic balancing strategy to improve the efficiency in the public Network environment.

I. INTRODUCTION

Over the last decade, researchers have studied how group communication applications like audio and video conferencing, multi-party games, content supply can be supported using IP Multicast [4]. However, over ten years after its initial proposal, IP Multicast is yet to be widely deployed due to fundamental concerns related to scalability, and support for higher layer functionality like reliability and congestion control. Recently, there has been a reevaluation by the research community of whether IP is indeed the right layer to support multicast-routing related functionality. A growing number of researchers [2, 3, 6, 9] have advocated an alternate architecture, where all multicast related functionality, including group management and packet replication, is implemented at end systems. We refer to such architecture as End System Multicast. In this architecture, end systems participating in a multicast group self-organize into an overlay structure using a completely distributed protocol. Further, end systems attempt to optimize the efficiency of the overlay by adapting to network dynamics and considering application level performance.

The rapid development of broadband technologies and the advancement of high-speed wired/wireless networks, the popularity of real-time video streaming applications and services over the Internet have increased by leaps and bounds. real-time video streaming communications such as web conference in intercompany networks or via Internet with virtual private networks (VPNs) are being widely deployed in a large number of corporations as a powerful means of efficiently promoting business activities without additional costs .A crucial concern in video streaming services is the protection of the bit stream from unauthorized use. We evaluate our techniques by testing the redesigned Narada protocol on a wide-area test-bed. Our test-bed comprises twenty machines that are distributed around North America, Asia and Europe. Our results demonstrate that our techniques can provide good performance, both from the application perspective and from the network perspective. With our scheme, the end-to-end bandwidth and latency attained by each receiver along the overlay is comparable to the bandwidth and latency of the unicast path from the source to that receiver. Further, when our techniques are incorporated into Narada, applications can see improvements of over 30–40% in both throughput, and latency.

II. WIRELESS NETWORK

Wireless networks (WNs) have gained a great deal of attention in the past decade due to their wide range of application areas. In general, wireless networks consist of low-cost, resource-constrained, distributed nodes, which usually scatter in the surveillance, working without attendance. If the operation is hostile, safety mechanisms against adversaries should be taken into consideration. If the node clone is a serious and dangerous one when to many physical attack. Because of production expense limitation, nodes are generally short of tamper-resistance hardware ,thus, to capture a few nodes, and to extract code, those materials to clone many nodes out of the hardware. Those cloned nodes that seem legitimate can freely join the network and then significantly enlarge the adversary's capacities to manipulate the network maliciously.

III. DISTRIBUTED SYSTEM

Distributed system is a field of computer science that studies distributed systems. A software system in which components located on networked method computers to communicate and coordinate their actions. The system should be interact with each other in order to achieve.

Three characteristics of distributed systems are: concurrency, lack of a global clock, and independent failure. The distributed systems differ from SOA-based on systems to massively multiplayer online games to peer-to-peer applications.

IV. EXAMPLES

The server traffic method includes the following:

Telecommunication networks:

- Mobile nodes and cellular networks
- System such as the Internet
- Wireless/wired networks
- map-reading algorithms

V. PROPOSED SYSTEM

- Traffic balancing schemes depending on whether the system dynamics are important can be either static and dynamic. Static schemes do not use the system information and are less complex while dynamic schemes will bring additional costs for the system but can change as the system status changes.

- The model has a main controller and balancers to gather and analyze. Thus, the dynamic control has little impudence on the other working nodes. The system to provide a basis for choosing the right Traffic balancing strategy.

- Thus, this model divides the public Network into several Networks. When the environment is very large and complex, these divisions simplify the Traffic balancing. The Network has a main controller that chooses the suitable s for arriving jobs while the balancer for each Network chooses the best Traffic balancing strategy.

A. Proposed Technique:

1. Best Partition Searching algorithm

The network partition balancer gathers load information from every node. This each node's load status is very important. The first work is to define the load degree of that nodes. The node load degree is related to various static parameters and dynamic parameters.

2. Round robin scheduling algorithm

Another balancing algorithms, which passes each new request to the next server. Before to start the Round Robin step, the nodes in the load balancing table are ordered. The system builds a circular queue and walks through the queue repetly. Jobs will then be assigned to nodes with low load degrees.

If a job arrives at the network partition, it will bring the inconsistent problem.

The system status will have changed but the information will still be old. This may lead to an load strategy nodes order. To resolve this problem, two Load Status Tables should be created as: Load Status 1 and Load Status 2. A flag is also assigned to each table to

indicate Read or Write. When the flag = "Read", then the Round Robin based on the load degree evaluation algorithm is using this table.

When the flag = "Write", the table is recharged, new information is written into this table. while the other is being prepared with the updated information. Once the data is refreshed, the table flag is changed to "Read" and the other table's flag is changed to "Write".

VI. Advantages

- Traffic balancing schemes depending on whether the system dynamics are important can be either static and dynamic.
- Static method does use the system information

ARCHITECTURE

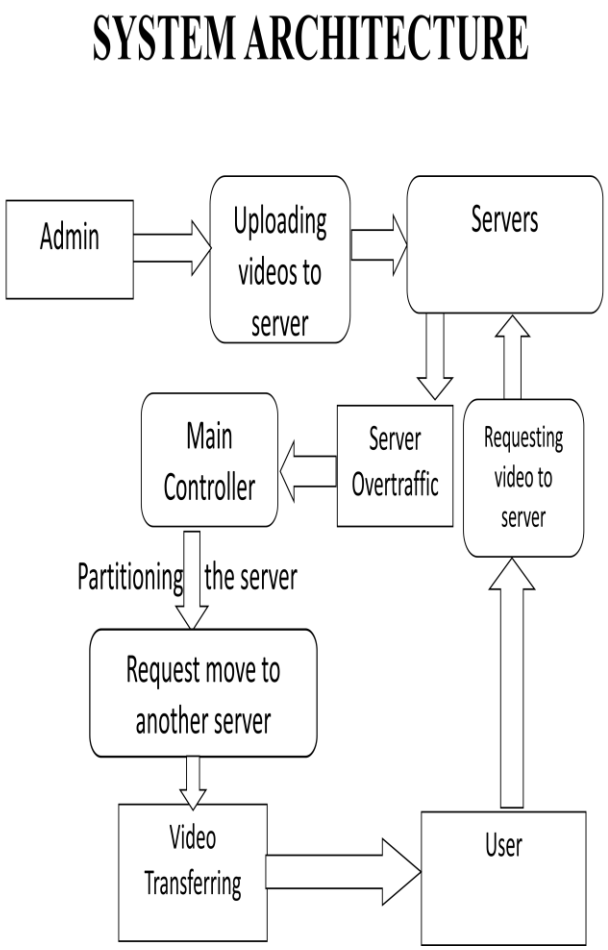

Fig.1.proposed architecture

VII. IMPLEMENTATION

Strategy to describe in detail

There are four modules are used in these method. Such as, Admin module, System module, Main controller and balancer, Network Traffic balancing

1. Admin Module

In this module, Admin user having login manages the detail which is presented in the network system. Admin securely handle the video transferring in network server by login into homepage.

2. System Model

A public Network is based on the standard wireless network model, with service provided by a service provider. A large public Network will include many nodes and the nodes in different geographical locations. Networking is used to manage this large Network. A Network is a subarea of the public Network with divisions based on the geographic locations. the main controller deciding which Network should receive the job. The load balancer then decides how to assign the jobs to the nodes. When the load status of a Network is normal, this can be accomplished locally.

3. Main controller and balancers

The load balance solution is done by the main controller and the balancers. first assigns jobs to the suitable Network and then communicates with the balancers in each to refresh this status information. Since it deals with information for each , smaller data sets will lead to the higher processing rates. The balancers in each gather the status information from every node and then choose the right strategy to distribute the jobs.

4. Network Traffic balancing Strategy

When the Network is idle, many computing resources are available and relatively few jobs are arriving. In this situation, this Network has the ability to process jobs as quickly as possible. There are many simple load balance algorithm methods such as Weight Round Robin algorithm, the and the Dynamic Round Robin the Round Robin algorithm is used here for its simplicity.

VIII. CONCLUSION

Focus of this paper is to develop an effective traffic balancing algorithm using round robin optimization technique to maximize or minimize different performance Delay or network load for the networks of different sizes. The proposed method allows flexible and accurate streaming content leakage detection independent of the length.

IX. FUTURE ENHANCEMENT

A better load status evaluation: A good algorithm is needed to set Load degree high and low, and the evaluation mechanism needs to be more comprehensive. Find other load balance strategy: so tests are needed to compare different strategies

REFERENCES

[1] Y. Chu, S.G. Rao, S. Seshan, and H. Zhang, "Enabling Conferencing Applications on the Internet Using an Overlay Multicast Architecture," Proc. ACM SIGCOMM, pp. 55-67, Aug. 2001.
[2] E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in Digital Video Content Protection," Proc. IEEE, vol. 93, no. 1, pp. 171-183, Jan. 2005.
[3] Y. Liu, Y. Guo, and C. Liang, "A Survey on Peer-to-Peer Video Streaming Systems," Peer-to-Peer Networking and Applications, vol. 1, no. 1, pp. 18-28, Mar. 2008.
[4] O. Adeyinka, "Analysis of IPSec VPNs Performance in A Multimedia Environment," School of Computing and Technology, University of East London.
[5] E.I. Lin, A.M. Eskicioglu, R.L. Lagendijk, and E.J. Delp, "Advances in digital video content protection," Proc. IEEE, vol.93, no.1, pp.171-183, Jan. 2005
[6] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," IEEE J. Sel. Areas Commun., vol.16, no.4, pp.573- 586, May 1998.
[7] M. Barni and F. Bartolini, "Data hiding for fighting piracy," IEEE Signal Process. Mag., vol.21, no.2, pp.28-39, Mar. 2004.
[8] K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility for collusion-resistant digital video watermarking," IEEE Trans. Multimedia, vol.7, no.1, pp.43-51, Feb. 2005.

