An Optimized Secure Key Exchange and Traffic Free Data Transmissionand Reception with Load Balancing Algorithm

R. Pitchandi[1], H. Jagadeesan[2]

[1]*Associate Professor,* [2]*Final Year MCA Student*

Department of Computer Applications, Madha Engineering College, Chennai, India

Abstract - The definition and implementation of an effective law for load balancing in Content Delivery Networks (CDNs) basically faces lots of severe major problems.Security is having a good implication over the internet. The communication between sender and receiver needs common key to encrypt and decrypt the data. For Key exchange, in particular Deffie-Hellman Key Exchange (DHKE), is among the core cryptographic mechanism for ensuring network security. For key exchange over the internet both security and privacy are desired. This kind of key exchange protocols provides a certain level of privacy protectionand the major criteria underlying the evolution of a list of important industrial standards which is particularly witnessed by the IKE and SIGMA protocol. This results is then leveraged in order to devise a time continuous algorithm for load balancing is also reformulated in a time discrete version. Finally, the overall approach is validated by means of simulator.

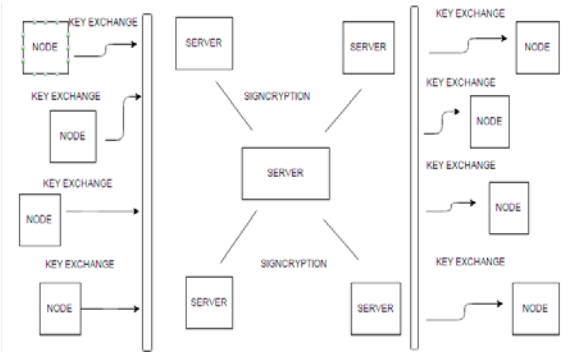
Keywords: Authenticated, Deniable, DHKE, DIKE, CDNs, IKE, Load balancing algorithm, Security, SIGMA.

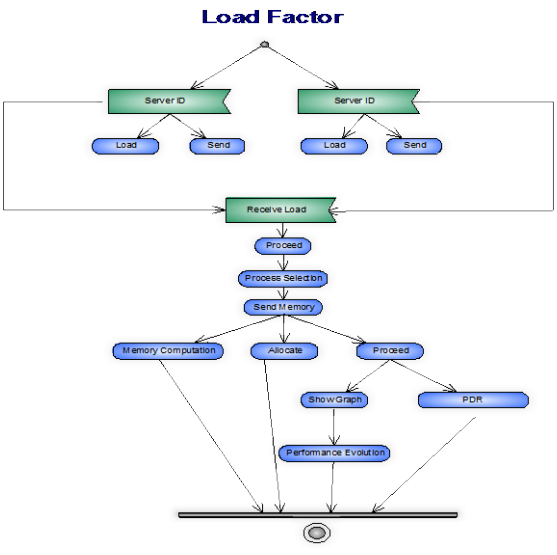
I. INTRODUCTION

In this paper we face the challenging issue of defining and implementing an effective law for load balancing in Content Delivery Networks. We base our proposal on a formal study of a CDN system, carried out through the exploitation of a fluid flow model characterization of the network of servers. Starting from such characterization, we derive and prove a lemma about the network queues equilibrium. This result is then leveraged in order to devise a novel distributed algorithm for load balancing. A Deniability service offered at the IP layer preserves the privacy feature from the upper layers. A Deniable authentication protocol is used to prevent the receiver from proving to a third party that the message is originated from the sender. The security of a communication protocol is based on one or more assumptions. A key agreement protocol is built on one or more cryptographic assumptions. A protocol with multiple independent assumptions with a logic OR relation is like a house with multiple outside doors with different security mechanisms. If the protocol has the more independent OR related assumptions then the attacker can try to attack the protocol in many ways. The overall approach is validated by means of simulations showing the effectiveness of the proposed algorithm in terms of both fair load distribution and limited service time. Authenticated key establishment is important for all the communication systems such as e-commerce, wireless, wired and Internet applications. This type of protocol is constructed using multiple cryptographic algorithms based on various cryptographic assumptions.

II. SYSTEM MODEL

This provides a comprehensive architectural overview of the system, using a number of different architectural views to depict different aspects of the system. It is intended to capture and convey the significant architectural decisions which have been made on the system.





III. PREVIOUS WORK

In a queue-adjustment strategy, the scheduler is located after the queue and just before the server. The scheduler might assign the request pulled out from the queue to either the local server or a remote server depending on the status of the system queues. In a rate-adjustment model, instead the scheduler is located just before the local queue: Upon arrival of a new request, the scheduler decides whether to assign it to the local queue or send it to a remote server. In a hybrid-adjustment strategy for load balancing, the scheduler is allowed to control both the incoming request rate at a node and the local queue length.Thus in Existing systems, Upon arrival of a new request, indeed, a CDN server can either elaborate locally the request or redirect it to other servers according to a certain decision rule, which is based on the state information exchanged by the servers. Such an approach limits state exchanging overhead to just local servers.

Demerits of previous work:

A critical component of CDN architecture is the request routing mechanism. It allows to direct users' requests for content to the appropriate server based on a specified set of parameters. The proximity principle, by means of which a request is always served by the server that is closest to the client, can sometimes fail. Indeed, the routing process associated with a request might take into account several parameters (like traffic load, bandwidth, and servers' computational capabilities) in order to provide the best performance in terms of time of service, delay, etc. Furthermore, an effective request routing mechanism should be able to face temporary, and potentially localized, high request rates (the so-called *flash crowds*) in order to avoid affecting the quality of service perceived by other users.

IV. PROPOSED METHODOLOGY

In a similar way, in this paper we first design a suitable load-balancing law that assures equilibrium of the queues in a balanced CDN by using a fluid flow model for the network of servers. Then, we discuss the most notable implementation issues associated with the proposed load-balancing strategy. A stronger form of deniability can be achieved using shared-key. Not a comprehensive approach big data. Inefficiency in incremental processing. A critical component of CDN architecture is the request routing mechanism. It allows to direct users' requests for content to the appropriate server based on a specified set of parameters.

We present a new mechanism for redirecting incoming client requests to the most appropriate server, thus balancing the overall system requests load. Our mechanism leverages local balancing in order to achieve global balancing. This is carried out through a periodic interaction among the system nodes.There are four different methods to invoke an OTcl command through the instance, tcl. They differ essentially in their calling arguments. Each function passes a string to the interpreter that then evaluates the string in a global context. These methods will return to the caller if the interpreter returns TCL_OK. On the other hand, if the interpreter returns TCL_ERROR, the methods will call tkerror{}.

Advantages of Proposed System:

The quality of our solution can be further appreciated by analysing the performance parameters.

The proposed mechanism also exhibits an excellent average Response Time, which is only comparable to the value obtained by the 2RC algorithm.

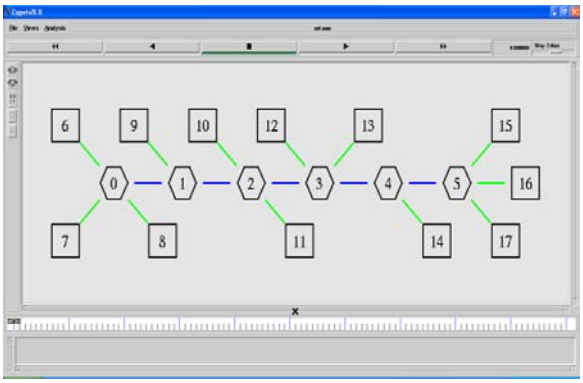
The excellent performance of our mechanism might be paid in terms of a significant number of redirections. Since the redirection process is common to all the algorithms analyzed, we exclusively evaluate the percentage of requests redirected more than once over the total number of requests generated.

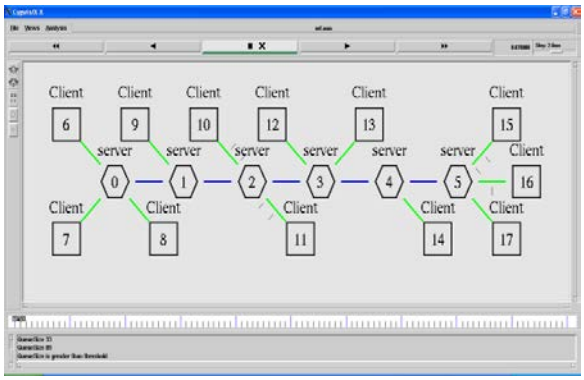
The data sent are transferred without any data damage or trafficless using security encryption and load balancing technique by using Network Simulator.

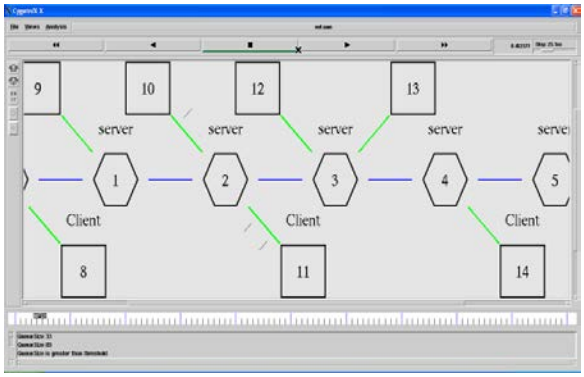
An effective request routing mechanism should be able to face temporary, and potentially localized, high request rates (the so-called flash crowds) in orderto avoid affecting the quality of service perceived by other users.

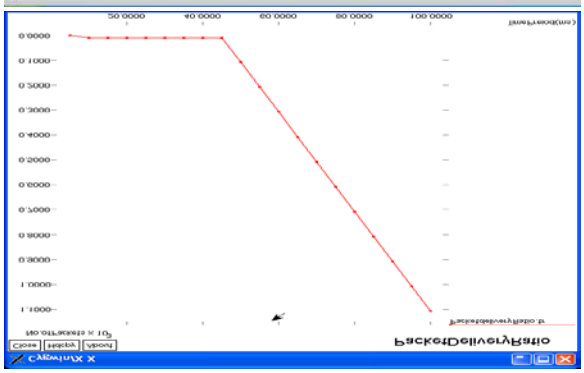
V. SIMULATION

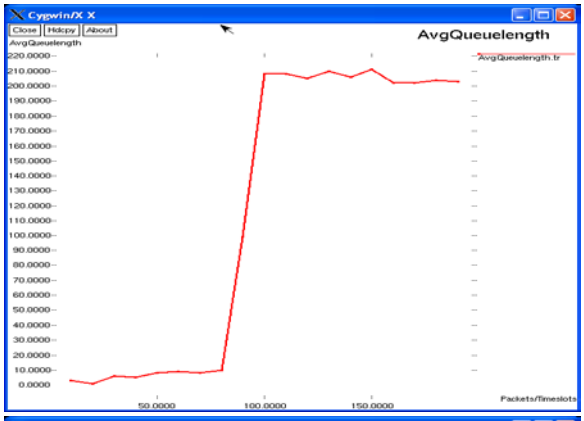
The data sent are transferred without any data damage or traffic less using security encryption and load balancing technique by using Network Simulator.

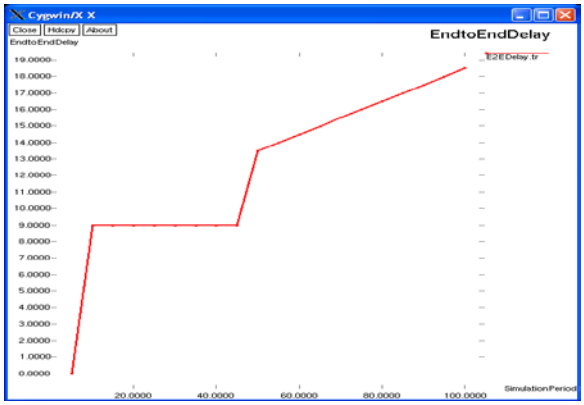












VI. CONCLUSION

We presented a novel load-balancing law for cooperative CDN networks. We first defined a model of such networks based on a fluid flow characterization. We hence moved to the definition of an algorithm that aims at achieving load balancing in the network by removing local queue instability conditions through redistribution of potential excess traffic to the set of neighbours of the congested server. The algorithm is first introduced in its time-continuous formulation and then put in a discrete version specifically conceived for its actual implementation and deployment in an operational scenario. Through the help of simulations, we demonstrated both the scalability and the effectiveness of our proposal, which outperforms most of the potential alternatives that have been proposed in the past. The present work represents for us a first step toward the realization of a complete solution for load balancing in a cooperative, distributed environment. Our future work will be devoted to the actual implementation of our solution in a real system, so to arrive at a first prototype of a load-balanced, cooperative CDN network to be used both as a proof-of-concept implementation of the results obtained through simulations and as a playground for further research in the more generic field of content-centric network management.

VII. FUTURE WORK

This work provides the secure and efficient technique of providing security between the sender and the receiver so that the data send by the sender should be made secure from various types of attacks such as de-synchronization attack, identity disclosure attack and spoofing attack. Signcryption offers a smaller message size and faster processing speed compared to sign-then-encrypt signature followed by encryption technique. Unlike safeguard that rely on symmetric key, the reliance of Signcryption on asymmetric cryptography makes non-repudiation possible. Sometimes due to network traffic and packet loss key unable to reach the destination point. At that time we can find out the some other path using the Graph Theory technique and resend the key to the receiver.

REFERENCES

[1] S. Manfredi, F. Oliviero, and S. P. Romano, “Distributed management for load balancing in content delivery networks,” in *Proc. IEEE GLOBECOM Workshop*, Miami, FL, Dec. 2010, pp. 579–583.

[2] H. Yin, X. Liu, G. Min, and C. Lin, “Content delivery networks: A Bridge between emerging applications and future IP networks,” *IEEE Netw.*, vol. 24, no. 4, pp. 52–56, Jul.–Aug. 2010.

[3] J. D. Pineda and C. P. Salvador, "On using content delivery networks to improve MOG performance," *Int. J. Adv. Media Commun.*, vol. 4, no. 2, pp. 182–201, Mar. 2010.

[4] D. D. Sorte,M. Femminella, A. Parisi, andG. Reali, "Network delivery of live events in a digital cinema scenario," in *Proc. ONDM*,Mar. 2008, pp. 1–6.

[5] Akamai, "Akamai," 2011 [Online]. Available: http://www.akamai. com/index.html

[6] Limelight Networks, "Limelight Networks," 2011 [Online]. Available: http://.uk.llnw.com

[7] CDNetworks, "CDNetworks," 2011 [Online]. Available: http:// www.us.cdnetworks.com/index.php

[8] Coral, "The Coral Content Distribution Network," 2004 [Online]. Available: http://www.coralcdn.org

[9] Network Systems Group, "Projects," Princeton University, Princeton, NJ, 2008 [Online]. Available: http://nsg.cs.princeton.edu/projects

[10] A. Barbir, B. Cain, and R. Nair, "Known content network (CN) request- routing mechanisms," IETF, RFC 3568 Internet Draft, Jul. 2003 [Online]. Available: http://tools.ietf.org/html/rfc3568

[11] T. Brisco, "DNS support for load balancing," IETF, RFC 1794 Internet Draft, Apr. 1995 [Online]. Available: http://www.faqs.org/rfcs/ rfc1794.html

[12] M. Colajanni, P. S. Yu, and D. M. Dias, "Analysis of task assignment policies in scalable distributedWeb-server systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 9, no. 6, pp. 585–600, Jun. 1998.

[13] D. M. Dias, W. Kish, R. Mukherjee, and R. Tewari, "A scalable and highly availableWeb server," in *Proc. IEEE Comput. Conf.*, Feb. 1996, pp. 85–92.

[14] C. V. Hollot, V. Misra,D. Towsley, andW.Gong, "Analysis and design of controllers for AQM routers supporting TCP flows," *IEEE Trans. Autom. Control*, vol. 47, no. 6, pp. 945–959, Jun. 2002.

[15] C. V. Hollot, V. Misra, D. Towsley, and W. bo Gong, "A control theoretic analysis of red," in *Proc. IEEE INFOCOM*, 2001, pp. 1510–1519.

[16] J. Aweya, M. Ouellette, and D. Y. Montuno, "A control theoretic approach to active queue management," *Comput. Netw.*, vol. 36, no. 2–3, pp. 203–235, Jul. 2001.

[17] F. Blanchini, R. L. Cigno, and R. Tempo, "Robust rate control for integrated services packet networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 5, pp. 644–652, Oct. 2002.

[18] V.Misra,W. Gong, W. bo Gong, and D. Towsley, "Fluid-based analysis of a network of AQM routers supporting TCP flows with an application to red," *Proc. ACM SIGCOMM*, pp. 151–160, 2000.

[19] D. Cavendish, M. Gerla, and S. Mascolo, "A control theoretical approach to congestion control in packet networks," *IEEE/ACM Trans. Netw.*, vol. 12, no. 5, pp. 893–906, Oct. 2004.

[20] V. Cardellini, E. Casalicchio, M. Colajanni, and P. S. Yu, "The state of the art in locally distributedWeb-server systems," *Comput. Surveys*, vol. 34, no. 2, pp. 263–311, Jun. 2002.

[21] Z. Zeng and B. Veeravalli, "Design and performance evaluation of queue-and-rate-adjustment dynamic load balancing policies for distributed networks," *IEEE Trans. Comput.*, vol. 55, no. 11, pp. 1410–1422, Nov. 2006.

[22] V. Cardellini, M. Colajanni, and P. S. Yu, "Request redirection algorithms for distributed Web systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 14, no. 4, pp. 355–368, Apr. 2003.

[23] M. Dahlin, "Interpreting stale load information," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 10, pp. 1033–1047, Oct. 2000.

[24] R. L. Carter and M. E. Crovella, "Server selection using dynamic path characterization in wide-area networks," in *Proc. IEEE INFOCOM*, Apr. 1997, vol. 3, pp. 1014–1021.

[25] M. D. Mitzenmacher, "The power of two choices in randomized load balancing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 12, no. 10, pp. 1094–1104, Oct. 2001.

[26] C.-M. Chen, Y. Ling, M. Pang, W. Chen, S. Cai, Y. Suwa, and O. Altintas, "Scalable request routing with next-neighbor load sharing in multi-server environments," in *Proc. IEEE Int. Conf. Adv. Inf. Netw. Appl.*, Mar. 2005, vol. 1, pp. 441–446.

[27] R. A. Horn and C. R. Johnson, *Topics inMatrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

[28] F. Cece, V. Formicola, F. Oliviero, and S. P. Romano, "An extended ns-2 for validation of load balancing algorithms in content delivery networks," in *Proc. 3rd ICST SIMUTools*, Malaga, Spain, Mar. 2010, pp. 32:1–32:6.

[29] P. Erdós and A. Rényi, "On the evolution of randomgraphs," *AMatematikalKutatóIntézetKóleményei*, vol. 5, pp. 17–61, 1960.

[30] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the internet topology," *Proc. SIGCOMM*, pp. 251–262, 1999.

[31] L. A. Adamic, R. M. Lukose, A. R. Puniyani, and B. A. Huberman, "Search in power-law networks," *Phys. Rev. E*, vol. 64, p. 046135, 2001.

[32] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.