ISSN:2231-0711

Novel WebEval in Content Delivery Networks (CDNs) Leakage in Numericable DNS flipped NetProV

T.Devi[1], O.Madhuri[2], S.Vandana[3]

1. Associate professor,I.T Department, VJIT,Hyderabad
2 .Assistant Professor,ECE Deparment,VJIT,Hyderabad
3. Assistant professor,I.T.Deopartment,VJIT,Hyderabad

***Abstract* --- A Content Delivery Network (CDN) is a content storage origin customer network, through an optimized and un-optimized connection across various parts of the globe through web, containing copied content in the cached servers, positions cached content to frequently requested customers. A CDN provides multi-client, routing & caching, delivery, security and scalability services to user's global content distribution networks. Most critical issues in multimedia content delivery in internet, public and private networks through content switching engine are transparent breakout, dropping, traffic shaping and leakage are due to content stream redundant zone, parallel reusable content distributor, high traffic routing clusters and indirect network non-transparent caching. In these issues, the most vulnerable is content leakage. Content Leakage in advanced high-speed wired/wireless web networks is due to the presence of unauthorized user presence in content location, duplicate content delivery and distribution of content replica. Content leakage detection methods evolved since, could not be able to address the solution for parallel reusable content distributors, which provides more content vulnerability in CDN. In this research work, a CDN Domain Name System (DNS) based Web Evaluation intelligence is proposed to resolve the web content leakage through maker agent server (MAS), flipped decision control traffic (FDCT) and Proxy Caching mechanisms (PCMs) to route multi-cast CDN web content. Our proposed method, limits vulnerable leakages in multiple CDNs through DNS flipped Net Provision Value Consistency (NPVC).**

Key Words - CDN, routing & caching, leakage, DNS, Proxy

I. INTRODUCTION

The purpose of content [3] delivery is to design the future of web world, guided by the principle architecture. To cope with the increasing need of content [1] [2] through web, network infrastructure deployed distributed network backbone (DNB) to cache the content and make it accessible from global locations in the web. These backbones have milti-global-locations to place the user client and server content. Distribution of content on these backbones uses the combination of data centres and cache based peer-to-peer centralized hosting networks. Some of these backbones are complicated with very network connectivity, providing large content to end-users. Most of the content delivery considers the network connectivity between content and the network, through internet traffic measurements. These traffic [4] measurements have shown, how volatile traffic can be. With the increase in user-content and shifts in content delivery , traffic volatility has become relevant. Handling changes in traffic, can be optimized by the utilization of data centres and residential ISPs networks and between large number of other networks and by optimizing the content flow in-and-out through their networks.

The CDNs deliver content from CDN work station to user location, due to the traffic measurements [7], *sudden leakage* [6] *may happen*, it is based on continuous monitoring of packet transition analysis, *content burst packets may get leaked*, it is based on throughput of the network and location of the burst is determined from the pressure analysis, *an algorithm for analysis of measurement of content leakage is to be derived*, it is based on the detection of content leakage and *a simulation of content leakage is implemented*, to solve the unpredicted leakage resulted numeric's.

This research work was initiated with a very broad objective-to improve the traffic measurements of content delivery through CDNs by utilising available resources and technology. The objectives of this research work is :

i. Explore the possibilities of content sever system traffic [4] [5] measurements,
ii. Content leakage detection and location in networks,
iii. Detection of content breaks,
iv. Find the technique that would utilize the existing measurements from the network in the most effective way,
v. Measure numerically, the state of the content leakage from the measured content and
vi. Analyse the possible implementation of these techniques in CDNs routers.

II. CONTENT DELIVERY NETWORKS (CDNS) LEAKAGE

A CDN reduces the redundancy in content flow through the networks, by making the single-content replica and serve the single-content replica available for many content users, which does not guarantee secure distribution of content. Content replica may get damaged due to integrity and modifying by any content required user or distributed network algorithms, this modified content may lead to leakage of content confidentiality to unauthorized parties.

The content delivery acts as a persistent caching mechanism, and used to implement in-network caching.

When content arrives, the router will initially query the content, in case of a cache hit, the router will direct the cache content. Otherwise, in other case cache content may get leakage in the network node, resulting in reduction of 'local hit ratio'.

User content request during the peak hours : content router delivery server system switches maximum, results in large energy consumption, large delays, and overhead problems could appear. Content routers should be designed to handle larger content cluster to avoid these overheads.

Although content can't be read directly, analysis of the content delivery leakage will infer user activity in networks.

III. CDN DOMAIN NAME SYSTEM (DNS) BASED WEB EVALUATION INTELLIGENCE

DNB is in general terms structured by the global internet, nobody has control over it, but each DNB has only control over its own network and able to interconnect with the other networks needed, under the control of multi-global-location domains intelligence system (IS). An IS is an autonomous administration rule, usually managed by an Interior Gateway Protocol (IGP) and Border Gateway Protocol (BGP). The greatest challenge for traffic measurements is to keep its DNB IS operate efficiently. The behaviour of DNB is dedicated to the end-users requesting content and the its operating choices. DNBs can resolve the problems of traffic measurements by performing application of technology and scientific principles to the measurements.

A. Content over Traffic Measurements

Traffic measurements contains multiple orders to perform content delivery without any Origin-Destination (OD) flows. It includes, content volume, traffic statistics from one network to another network, DNB configuration to simulate numerically the network behaviour. The goal of these numerical simulations is to find an DNB configuration that measures the traffic as early as possible.

Figure 1 shows, how an DNB Configuration can be used to numerically simulate the content traffic in networks. In starting the network, the OD inward flow path takes FOUR paths, they are, Content Work Station A-1-Distributed Router A-2-Router A-3-Terminal A-4-Router D-2-Router E-1-File Share-2-Router C-2-User, Content Work Station A-1-Distibuted Router A-1-Router B-2-Router C-3-User, Content Work Station B-2-Gateway A-1-rOUTER b-2-Router C-3-User and Content Work Station B-2-Gateway A-1-Router B- Distributed Router A-2-Router A-3-Terminal A-4-Router D-2-Router E-1-File Share-2-Router C-2-User. In the above four path, the best possible path is Content Work Station A-1-Distibuted Router A-1-Router B-2-Router C-3-User has accumulated total weight of 7.

The OD outward flow path takes FOUR paths, they are, User-1-Rouer C-1-Router B-1-Gateway A-2-Content Work Station B, User-1-Router C-3-File Share-2-Router E-3-Router D-1-Terminal A-5-Router A-3-Distributed Router A-1-Content Work Station A, User-1-Router C-3-File Share-2-Router E-3-Router D-1-Terminal A-5-Router A-3-Distributed Router A-2-Router B-1-Gateway A-2-Content Work Station B and User-1-Router C-1-Router B-Distributed Router A-1-Content Work Station A. In these, the best possible paths are User-1-Rouer C-1-Router B-1-Gateway A-2-Content Work Station B and User-1-Router C-1-Router B-Distributed Router A-1-Content Work Station A, has accumulated total weight of 5.

Here in this scenario, the total weight of OD outward flow gives conflicts between the traffic measurements, results in collision and leakage of content from User location to Content Work Station, to overcome these, we need a strategy.

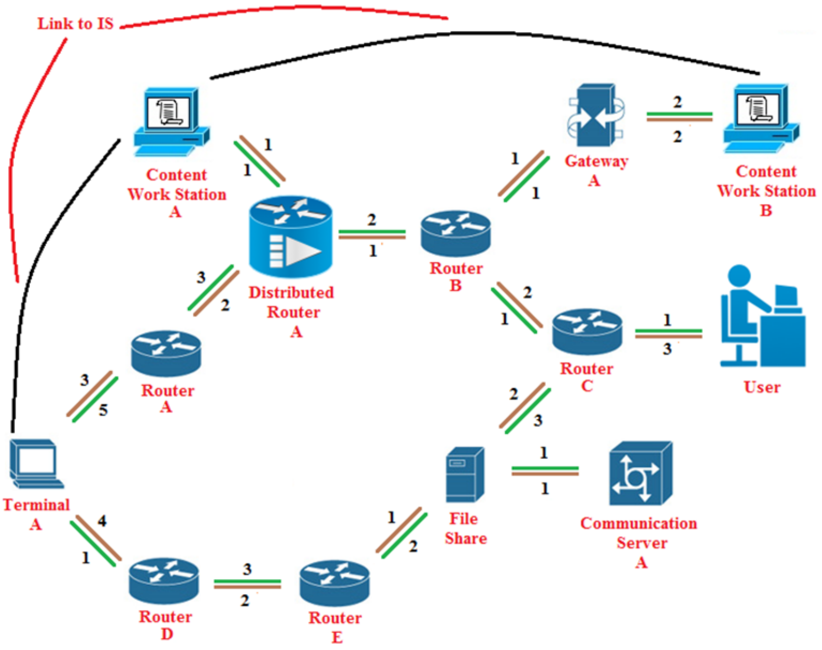

Figure 1: Traffic OD measurements

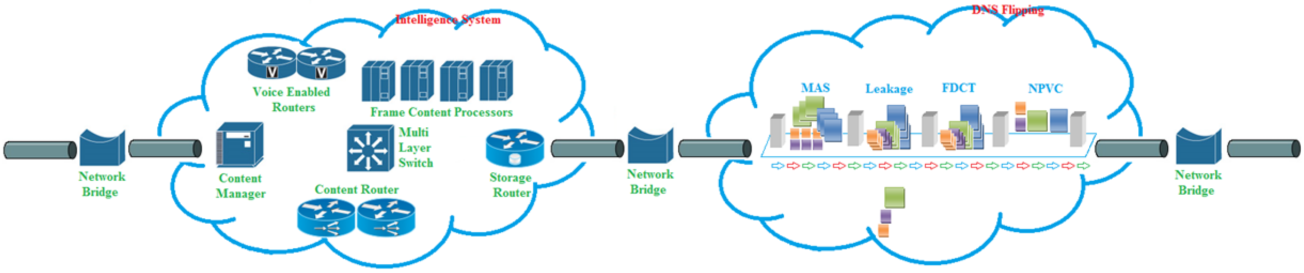

Figure 2 : DNB approach.

B.
Proposed Distributed Network Backbone (DNB)

DNB provides a solution to the collision and leakage of content from the networks, by routing the content through IS and DNS flipping approaches.

Figure 2 shows, how IS and DNS flipping approaches, used to avoid collision and leakage of content from networks.

Proposed DNB approach involves Intelligence System and DNS Flipping, involving objectives to i) change the statistics of network service from delivering the packets to a given destination content network, ii) to provide content by a given content user, iii) detect the content leakages and iv) estimate the content delivery.

1. Intelligence System (IS) Approach

Each node in DNB performs content forwarding by relying in the presence of the following :

i) Content Manager : It is responsible for tracking the cache content to list the interests, stores the content from which the interests were originally received, also to implement forward and reverse path forwarding: as soon as the router receives a Content Packet. It a) forwards the content on the same intelligence system, b) checks the content received, c) manages the content interest and d) deletes the content collision entry.

ii) Voice Enabled Routers : It is responsible to route voice content stored in Frame Control Processors. It acts as a voice catching storage for the node, and used in-networking caching. When request arrives, the router will initially manage voice content by routing the voice data content to user location.

iii) Content Router : It is responsible to route data content, based on user authorized locations and Content Router Layer (CRL). CRL is responsible for choosing the interest content packet, to forward or to reverse the data content on network interface. CRL is also responsible for data multicasting and data packet dropping based on NACK received.

iv) Frame Content Processors : DNB forces content packets to be published under a given frame, which cannot be changed. These frames are imposed to make sure that global in-networking caching always return the new content packet to register in the network. It supports content processing, the content received from the network, will be framed in to content packets, and a prefix is attached at the left most or right most of the content frame. Furthermore, it provides selectors for setting further conditions on interest content frames.

v) Storage Router : In order to optimize the content distribution performance of DNB, caching policy is implemented in Storage Router. In particular, the caching policies are, inclusion and decision policies.

An inclusion policy is used to select the content to be removed from a full cache, to store new cache and provide recently and frequently used cache.

The decision policy chooses a network wide cache, to choose the decision between new content and leave a content copy everywhere.

vi) Multi Layer Switch : It is content based security model, designed to respond to an interest by providing a user cached copy, check and verify the received cache, validate the content received and provide the relevance content satisfies the request originally sent by the user.

2. DNS Flipping Approach

DNS provides a name service for the proposed Intelligence System Internet. It is one of the largest name services in operation today, serves a highly diverse community of hosts, users, and networks and uses a unique combination of hierarchies, caching and datagram access. Our research work, provides an idea for the initial design of the DNS and examines the current implementation and usages.

The base design of our proposed DNS Flipping Approach is implemented through the following :

i) Maker agent server (MAS) : Our analysis of hostnames and their servers contains multiple servers in different locations. These servers use the services, of content delivery infrastructure, of DNS resolution, mapping of domain to content delivery, answering to the requested domains, return to server IP address of the requesting DNS server.

ii) Decision control traffic (DCT) : A DNS server has a decision control method, for content balancing across multiple servers. Decision control method has two principles :

a)Multi-decision control traffic : It provides multiple IP addresses with in a DNS server response. From a network perspective, this implies that, by taking the average number of IP addresses and subnets per DNS reply and content normalization by traffic volume requests.

b)Flipped-decision control traffic : It provides different IP addresses for repeated DNS server response. The second form of DNS is flipped based decision, it returns to different IP addresses for repeated contents to server diversity across time.

iii) Proxy Caching mechanisms (PCMs) : To understand the DNS load balancing, more IP addresses diversity is resolved to supply caches based on source IP address of the querying proxy cache. A possible solutions to the querying proxy cache is by the following mechanisms :

a)Proxy-Cast : It is a routing technique used to send content to the user router location. It is provided with multiple destination locations, selects the shortest route for the destination according to the conjunction, based on the routing weights content is routed and by overcoming the traffic mechanisms to its one of its locations.

b)DNS based Caching : When requesting a content, the user router asks a DNS Caching, to cache for the ISP domain name. DNS Cache asks for content authorized server based on the request comes from user content location, which is coming from DNS Caching server. Thus DNB selects only server based IP address of end user content.

iv)Net Provision Value Consistency (NPVC) : The NPVC Protocol incorporates a mechanism to redirect user content at the application level. By sending NPVC protocol through DNS web server to the end user content router, to tell the user a request object is available from the server.

IV. NOVEL WEB EVALUATION THROUGH DNS FLIPPED NET PROVISION VALUE CONSISTENCY (NPVC)

Proposed Novel WebEval relies on DNS and DNB through NPVC, network information is collected and processed by the DNS servers, which are ranked by the weight criteria, to optimize the delay between the end user and DNB. Today, there is no protocol to handle the above operations. Our Novel Web Evaluation provides solution to design, implement and evaluate a scalable system that can support DNS flipped NPVC.

The architecture of DNS flipped NPVC is shown in below figure 3.

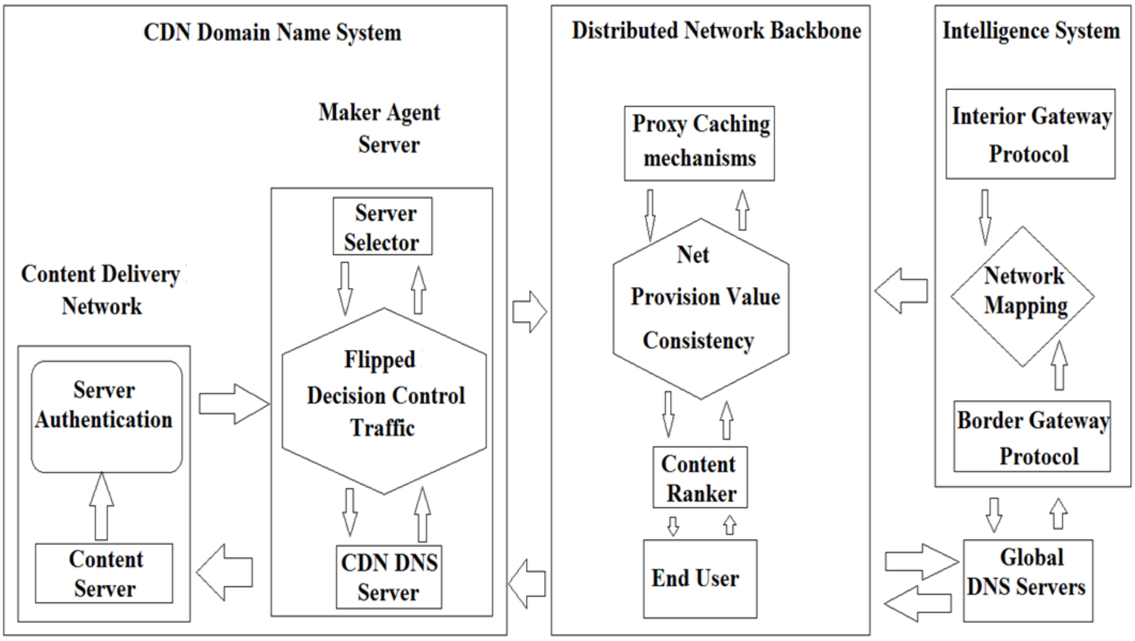

Figure 3 : The architecture of DNS flipped NPVC

The above architecture shown in figure 3, explains the implementation of CDN DNS based DNB providing content leakage detection and avoidance. Through the following approaches, we can evaluate the CDN leakages :

i. maintain an up-to-date annotated content of the DNS network and its properties,
ii. produce preference content ranking based on paths between end-users and servers,
iii. communicate with the CDN server selection to influence the end-user,
iv. gather information about the topology and state of the network,
v. routing information about the paths of the traffic,
vi. build an annotated network map of CDN DNS network towards fast lookup on path properties,
vii. weight based path or link component should be updated immediately,
viii. effected paths should recalculate the properties of weights,
ix. content ready for access ensure high throughput and
x. end-user request content from CDN DNS should not be vulnerable.

V. NUMERICAL ANALYSIS AND DISCUSSIONS

This section aims to compare the performance of feasible solution, as well as overall performance of the proposed approach. Numerical results shown in table 1, obtained from a large number of experiments showed that the performance of the proposed backbone approach 1, 2 and 3 is better.

Table 1 : Numerical analysis of the proposed approach.

	Content Size (Bytes)					DNB Result (%)					NPVC Result (%)		
Backbone Approach	Voice	Frame	Data	Cache	Load	Content Forward	Content backward	Content drop	Content Leakage	Time	Optimal	Leakage	Time(econds)
1	10	15	5	3	2	27	10	2	1	25s	15	4	102s
2	15	20	9	6	2	37	17	3	4	80s	19	9	342s
3	20	30	12	2	2	52	16	10	0	10s	22	2	48s

From the above numerical results, the proposed approach can mode above 90% total quality in content leakage detection, up to 40% of content deviation, with total 80% of utility for content time recovery as high as 70 %. This means that the proposed approach is optimized in useful approach, as it is solving the content leakage approaches and can be solved effectively. Local optimization, on the other hand, can achieve comparable results for high content leakage recovery (up to 95%)

VI. CONCLUSIONS

The live content streaming using DNB DNS and NPVC investigates on the content has given solution to leakage problems. With this class of approaches, we envisage that virtual DNS server would function as DNB for IS, content processing node and multicast node. A DNB considers not only front end servers but also backend servers, links and content distribution trees and become substantial to the previous considerations. We have addressed the challenge by approaching a DNS model that determines optimal NPVC and link configuration, with content distribution from servers to user router. We went on developing an approach to Web Evaluation based on DNB and NPVC, that could find near optimal solution to CDN leakage in networks. Numerical results showed that the proposed approach is able to achieve solution accuracy (above 70 %) for large content leakage with computation time.

REFERENCES

[1]. C.-S. Yang and M.-Y. Luo, “An effective mechanism for supporting content-based routing in scalable Web server clusters,” *Proc. International Workshop on Parallel Processing (ICPP’99)*, pp. 240-245, IEEE CS Press, Los Alamitos, CA, USA, 1999.

[2]. D. Agrawal, J. Giles, and D. C. Verma, “On the performance of content distribution networks,” *Proc. International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'01)*, The Society for Modeling and Simulation International (SCS), 2001.

[3]. 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.

[4]. Golaup, and H. Aghvami, “A multimedia traffic modeling framework for simulation-based performance evaluation studies,” Computer Network, vol. 50, no. 12, pp. 2071-2087, 2006.

[5]. S. Amarasing and M. Lertwatechakul, “The Study of Streaming Traffic behavior,” KKU Engineering Journal, vol.33, no.5, pp.541-553, Sept.- Oct. 2006.

[6]. Atsushi Asano, Hiroki Nishiyama, and Nei Kato, “The Effect of Packet Reordering and Encrypted Traffic on Streaming Content Leakage Detection (Invited Paper),” International Conference on Computer Communication Networks 2010 (ICCCN 2010), Zurich, Switzerland, Aug. 2010.

[7]. K. Matsuda, H. Nakayama, and N. Kato, “A Study on Streaming Video Detection using Dynamic Traffic Pattern,” IEICE Transactions on Communications (Japanese Edition), vol.J19-B, no.02, 2010.