Blocking Misbehaving Users and Error Correction Method in Nymble Secure System

[1]A. Thirupathaiah, [2]K. Eswar, [3]Dr. P. Harini

[1,2,3]Dept. of CSE, St. Ann's College of Engineering & Technology, AP, India

Abstract

Packet loss and end-to-end delay limit delay sensitive applications over the best effort packet switched networks such as the Internet. In the system Nymble, a system in which servers can “blacklist” misbehaving users, thereby blocking users without compromising their anonymity. Thus agnostic to different servers definitions of misbehavior where servers can blacklist users. But according to our calculation there is a LOP (loss of packets) and DON (delay of network) can happen while blacklisting the misbehavior users from all the corners of the websites. To overcome the loss we propose PDF (path diversity with forward error correction technique) system for delay sensitive applications over the Internet in which, disjoint paths from a sender to a receiver are created using a collection of relay nodes along with the Nymble approach. A scalable, heuristic scheme for selecting a redundant path between a sender and a receiver, and show that substantial reduction in packet loss can be achieved by dividing packets between the default path and the redundant path. NS simulations are used to verify the effectiveness of PDF system.

Keywords

NYMBLE, PDF, LOP, DON, NS

I. Introduction

There are several solutions to this problem, each providing some degree of accountability. In pseudonymous credential systems users log into websites using pseudonyms, which can be added to a blacklist if a user misbehaves. Unfortunately, this approach results in pseudonymity for all users, and weakens the anonymity provided by the anonymizing network.Anonymous credential systems employ group signatures. Basic group signatures allow servers to revoke a misbehaving user’s anonymity by complaining to a group manager. Servers must query the group manager for every authentication, and thus lacks scalability. Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced; such an approach does not provide the backward unlinkability that we desire, where a user’s accesses before the complaint remain anonymous. Backward unlinkability allows for what we call subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, approaches without backward unlinkability need to pay careful attention to when and why a user must have all their connections linked, and users must worry about whether their behaviors will be judged fairly.

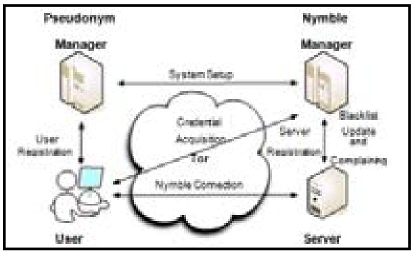


Fig. 1: The Nymble System Architecture Showing the Various Modes of Interaction

Delay sensitive applications such as video streaming and conferencing are challenging to deploy over the Internet due to a number of factors such as, high bit rates, delay, and loss sensitivity. Transport protocols such as TCP are not suitable for delay sensitive applications since they retransmit lost packets, resulting in long delay. To this end, many solutions have been proposed from different perspectives. From source coding perspective, layered and error-resilient video code cs have been proposed. A layered video codec deals with heterogeneity and time-varying nature of the Internet by adapting its bit rate to the available bandwidth [1]. An error-resilient codec modifies the bit stream in such a way that the decoded video degrades more gracefully in lossy environments[2-3]. From channel coding perspective, Forward Error Correction (FEC) techniques have been proposed to reduce delay due to re- transmission, at the expense of bandwidth expansion [4-5]. Another commonly used technique in lossy environments is retransmission. While retransmission results in the least amount of bandwidth overhead, it does introduce additional delay of roughly a round trip time between the sender andreceiver. Hence, the overall delay using retransmissions often exceeds 150 milliseconds, the tolerable delay limit for many interactive applications such as video conferencing [6]. From protocol perspective, TCP-friendly protocols [1, 7] use equation based rate control to compete fairly with other TCP traffic for bandwidth, while stabilizing the throughput, and reducing jitter for multimedia streaming [7]. From network perspective, Content Delivery Network (CDN) companies such as Akamai use edge architecture as shown in Figure 1 to achieve better load balancing, lower latency, and higher throughput. Edge architecture reduces latency by moving content to the edge of the network in order to reduce round-trip time and to avoid congestion in the Internet.

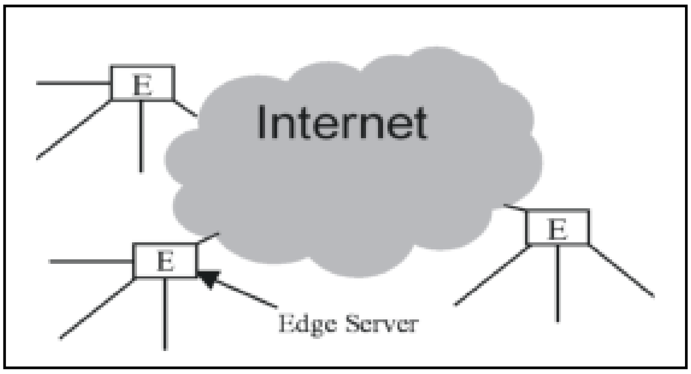


Fig. 2. Edge Server Architecture

Most of the above schemes assume a single fixed path between the receiver and the sender throughout the session. If the network is congested along that path, video streaming suffers from high loss rate and jitter. Furthermore, authors in [8-9] have revealed the ill-behaved systematic properties in Internet routing, which can lead to sub-optimal routing paths. Based on these, it is conceivable to send packets simultaneously over multiple paths as a diversification scheme to combat the unpredictability and congestion in the Internet. If the path between a particular sender and a receiver experiences packet loss due to congestion, packets traversed through other paths can be used to recover the lost packets. In previous work [10], we have shown that by sending packets at appropriate rates on the disjoint paths from multiple senders to the receiver, and by employing redundancy through FEC, the effective packet loss rate can be significantly reduced as compared to sending all packets on a single path with the same level of redundancy. In essence we have shown that path diversity transforms a single path with bursty loss behavior into multiple paths with uniform loss for which FEC is quite effective.

In this paper, we extend our previous work to propose a single sender, single receiver, Path Diversification system with Forward error correction (PDF), over packet switched networks such as the Internet. Our proposed PDF system is similar to Resilient Overlay Network (RON) [11] in that it consists of a set of participating nodes that receive and forward packets to other nodes. Unlike RON however, our PDF system forwards packets simultaneously over multiple redundant paths rather than selecting an optimal path to send all the packets on. If the packet loss between multiple paths are correlated, path diversity and FEC are not enough to bring packet loss rate down to acceptable levels. Hence, the central question in one sender one receiver scenario with path diversity is whether there exists sufficiently disjoint paths between a pair of senders and receivers on the Internet to result in uncorrelated loss patterns between paths. If the paths are not entirely disjoint, then the probability of congestion on the shared links between the paths must be small in order to minimize the overall end-to-end loss.RON, has shown how to route packets around all the observed outages between any pair of senders and receivers in an experimental network. This suggests the existence of path redundancy between nodes on the Internet. Many Internet topological models such as Albert-Barabasi [12] also exhibit a high level of disjointness between the paths connecting two nodes. In this paper, we propose a heuristic scheme to create a redundant path using the overlay framework.We further characterize the disjointness between the redundant and default paths for various Internet topologies, and show significant reduction in packet loss using PDF system over uni-path scheme [13]

II. Model

Path diversity using overlay networks has been proposed. To create a redundant path in the overlay framework, the sender sends packets to a relay node, and the relay node then forwards packets to the receiver By selecting the relay node appropriately, the packets traveling through the relay node take a different underlying physical path than that of the Internet default path between the sender and receiver. Hence, path diversity is accomplished by sending packets on both the default path and the redundant path. From traffic engineering point of view, RON also provides alternate paths between sender and receiver using relay nodes. However, RON actively probes for the current "best" path based on delay and loss, and sends all packets through that path rather than simultaneously sending packets on multiple paths. Note that path diversity can also be created using source based routing supported at the routers. Using this approach, one can explicitly specify a set of nodes for each packet to transverse to the destination. Currently, source based routing is available only to a few Autonomous Systems (AS).

Many diversity schemes have been proposed in wireless literature, ranging from frequency and time, to spatial diversity. In wired networks, path diversity was first proposed in the theoretical work on information dispersion for security and load balancing was proposed. There have been other works dealing with simultaneous downloading of data from multiple mirror sites to accomplish path diversity. If the data is not delay sensitive, it is possible to use multiple TCP connections to different sites, with each TCP connection downloading a different part of the data. For example, Digital Fountain has used an advanced class of linear-time codes to enable the receivers to receive any N linear-time coded packets. The effect of sending packets at a lower rate on multiple independent paths in effect transforms the bursty loss into a uniform loss, thus increasing the efficiency of FEC techniques. Naturally, given a number of independent paths each with a different loss behavior, the source bit rate, and the total amount of FEC protection, there should be an optimum partition of sending rates for each path in order to minimize the irrecoverable loss probability. The irrecoverable loss probability is the probability that FEC cannot recover the lost packets in a FEC block. For a Reed-Solomon code RS(N,K) which contains K data packets and N − K redundant packets, the irrecoverable loss probability is the probability that more than N −K are lost per N packets. In our previous work , we have provided a procedure for computing the optimal sending rates for different paths from multiple senders to one receiver in order to minimize the irrecoverable loss probability. We now present the numerical results based on our previous work to motivate the problem and approach for this paper.

Let us consider sending packets on two disjoint paths A and B. Packets are protected using RS(30, 23), packet size is 500 bytes, and total sending rate is 800 kbps. We refer to the "average bad time" as the average duration that the path is in "bad" state or in congestion, and the "average good time" as the average duration that the path is in "good" state or without congestion. The longer average bad time indicates longer burst loss. The average good time for both paths is 1 second. The average bad time for path A is 10 milliseconds, while that of path B varies from 10 milliseconds to 50 milliseconds as shown in Figure 2. Figure 2 shows N, the optimal number of packets per FEC block that should be sent on path A, or equivalently, sending rate on path A as a function of the average bad time of path B. As seen, when the average good and bad times of the two paths are identical at 1 second and 10 milliseconds respectively, packets are divided equally between them at 15 packets each.

When the average bad time of path B increases, more packets are sent on path A. This is intuitively plausible since path A is a better path. Figure 3&4 shows the ratio of irrecoverable loss probability by sending all packets on path A, the better path, over that of optimally dividing packets between paths A and B. As seen, the irrecoverable loss probability using path diversity can be reduced as much as 15 times over that of using uni-path scheme. An important observation to be made is that even though the average loss rate of path B is roughly 5%, i.e. five times than that of path A, protecting packets with RS(30,23) and sending packets simultaneously over both paths, can still reduce the irrecoverable loss probability. This suggests that if there exists a redundant path which is not "nearly" as good as the default path between sender and receiver, then it is still advantageous to deploy the path diversity scheme. Further quantitative results on amount of FEC and burstiness of the network.

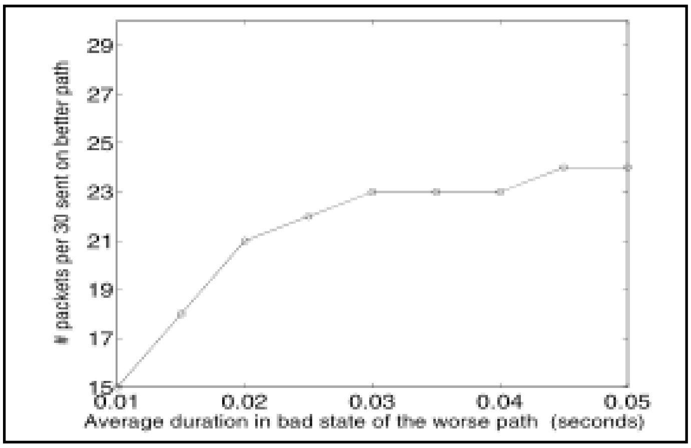


Fig. 3: Optimal Rate Partition Using Two Paths

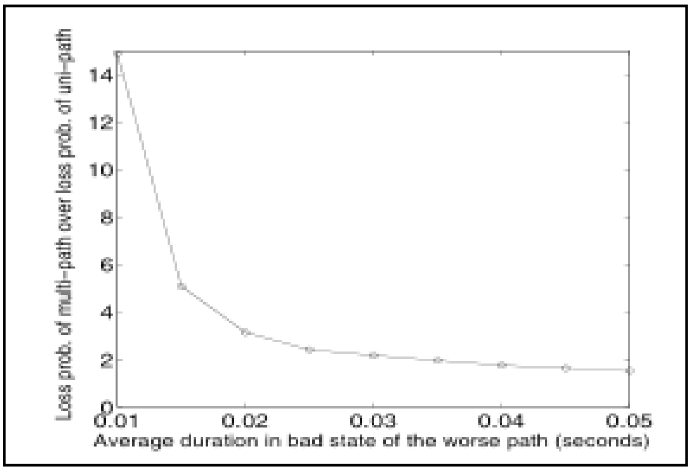


Fig 4: Ratio of Irrecoverable Loss Probabilities of the Uni-Path Scheme to Multi-Path Scheme

III. Security Analysis

Theorem 1: Our Nymble construction has Blacklistability, Rate-limiting, Non frameability and Anonymity provided that the trust assumptions hold true, and the cryptographic primitives used are secure.

We summarize the proof of Theorem 1. Please refer to our technical report for a detailed version.

A. Blacklistability

An honest PM and NM will issue a coalition of c unique users at most c valid credentials for a given server. Because of the security of HMAC, only the NM can issue valid tickets, and for any time period the coalition has at most c valid tickets, and can thus make at most c connections to the server in any time period regardless of the server's blacklisting. It suffices to show that if each of the c users has been blacklisted in some previous time period of the current linkability window, the coalition cannot authenticate in the current time period k.

Assume the contrary that connection establishment k using one of the coalition members' ticket was successful even though the user was blacklisted in a previous time period k′. Since connection establishments k′ and k were successful, the corresponding tickets ticket′ and ticket must be valid. Assuming the security of digital signatures and HMAC, an honest server can always contact an honest NM with a valid ticket and the NM will successfully terminate during the blacklist update. Since the server blacklisted the valid ticket ′ and updates its linking list honestly, the Server Link Ticket will return fail on input ticket , and thus the connection k must fail, which is a contradiction.

B. Non-Frameability

Assume the contrary that the adversary successfully framed honest user i with respect to an honest server in time period t, and thus user i was unable to connect in time period t using ticket even though none of his tickets were previously blacklisted. Because of the security of HMAC, and since the PM and NM are honest, the adversary cannot forge tickets for user i, and the server cannot already have seen ticket; it must be that ticket was linked to an entry in the linking list. Thus there exists an entry (seed , nymble) in the server's linking list, such that the nymble in ticket equals nymble. The server must have obtained this entry in a successful blacklist update for some valid ticket b, implying the NM had created this ticket for some user i.

Ifi=i, then user˜i's seed 0 is different from user i's seed .so long as the PM is honest, and yet the two seed 0's evolve to the same seed , which contradicts the collision- resistance property of the evolution function. Thus we have i = i. But as already argued, the adversary cannot forge i's ticket b, and it must be the case that i's ticket b was blacklisted before t, which contradicts our assumption that i was a legitimate user in time t.

C. System Description

The system architecture for path diversity based on overlay framework. As seen in Figure 5, the system consists of a set of participating nodes. Circles represent participating overlay nodes, squares denote routers, and the bold solid and dashed lines represent the underlying physical and virtual paths between the nodes respectively. The thin vertical solid lines connecting circles and squares represent the correspondence between virtual nodes and physical routers. At any instance, a node can act simultaneously as a receiver, a sender, or a relay node. A sender can send video packets to the receiver using the default Internet path or via a relay node which then forwards the video packets to the receiver. By choosing an appropriate relay node, the packets traverse an underlying physical path that is different from the one used by default Internet path. Nodes can be deployed at various locations on the Internet, although redundant paths via nodes in the same AS may have larger number of shared links. Hence, nodes are preferably located in different AS to reduce correlated congestion and outages so as to improve the performance of the PDF system.

A participating node which is neither a receiver nor a sender, may still receive and forward packets on behalf of other senders and receivers. For two way applications such as video conferencing, they act simultaneously as both senders and receivers. In addition, the senders and receivers do not necessarily have to be the participating nodes. We envision the participating nodes as an overlay network to be deployed by companies or organizations that are interested in providing low delay communication services such as video streaming or conferencing over the Internet between their geographically diverse sites. Companies and organizations typically have multiple gateways from their ASes to other ASes that potentially enable large number of independent paths.

We use UDP to send all packets between participating nodes since TCP is not appropriate for real-time data transmission due to its variable throughput, and lack of precise rate control. In addition, one of the main concerns with using multiple paths to send packets is that packets likely arrive at the destination out of order. For UDP traffic, this is not a concern since a reordering buffer at the receiver can be used. For TCP traffic, however, out-of-order packets are treated as packet loss, and TCP fast retransmit algorithm continually resends packets which are merely in transit, reducing the connection bandwidth. One major difference between our PDF system and RON is that RON dynamically determines the "best" path to send all packets on, while our PDF system sends packets simultaneously on multiple paths, similar to Detour.

Detour however, uses the multi-path at the router level whereas we accomplish multi paths at the application level, allowing the flexibility to send packets at different rates on different paths to the destination.

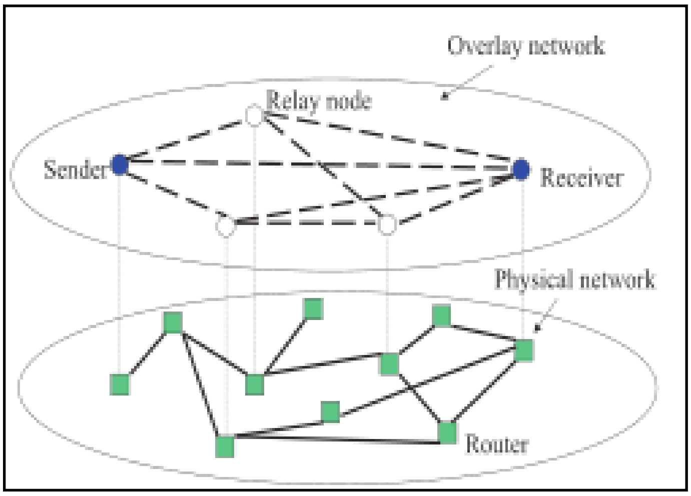


Fig. 5: System Architecture; Bold Dashed and Solid Lines Denote Virtual and Physical Paths

IV. Motivation

IP-address blocking By picking IP addresses as the resource for limiting the Sybil attack, our current implementation closely mimics IP-address blocking employed by Internet services. There are, however, some inherent limitations to using IP addresses as the scarce resource. If a user can obtain multiple addresses she can circumvent both nymble-based and regular IP-address blocking. Subnet-based blocking alleviates this problem, and while it is possible to modify our system to support subnet-based blocking.

Server-specific linkability windows An enhancement would be to provide support to vary T and L for different servers. As described, our system does not support varying linkability windows, but does support varying time periods. This is because the PM is not aware of the server the user wishes to connect to, yet it must issue pseudonyms specific to a linkability window. We do note that the use of resources such as client puzzles or e-cash would eliminate the need for a PM, and users could obtain Nymbles directly from the NM. In that case, server-specific linkability windows could be used.

Side-channel attacks While our current implementation does not fully protect against side channel attacks, we mitigate the risks. We have implemented various algorithms in a way that their execution time leaks little information that cannot already be inferred from the algorithm's output. Also, since a confidential channel does not hide the size of the communication, we have constructed the protocols so that each kind of protocol message is of the same size regardless of the identity or current legitimacy of the user.

A. Redundant Path Selection

In this section, we propose a scalable, heuristic method for finding a redundant path via a participating relay node. Selecting an optimal path between a pair of nodes on the Internet at any one instant is difficult and complex. If the traffic conditions of the path vary rapidly, the problem becomes almost infeasible. For scalability reasons, the Internet domain routing is handled primarily by the Border Gate Protocol (BGP). BGP only exchanges and updates summarized information between ASes, ignoring the link usages and topologies within ASes. Hence, accurate path information such as number of links along the path and their associated latencies can not be obtained through BGP. Other link state routing protocols such as Open Shortest Path First (OSPF) periodically probe the links between the routers for updated information such as latency, bandwidth, and link failures. OSPF can provide these information reasonably accurately,however, it is not scalable and therefore, is only used within ASes.

To measure end-to-end latency, bandwidth, and packet loss between nodes at various locations on the Internet, probing tools can be used at the expense of bandwidth expansion due to sending probed packets.

Another approach is to use passive probing in which the application packets themselves are used as the probing packets, to determine the packet loss rate, latency, and bandwidth. The advantage of this approach is lack of bandwidth expansion; however, its drawback is that the measurement process depends on the application sending rates. If an application sends packets at a slow rate, the measurement resolution is low, resulting in inaccurate end-to-end estimates of packet loss rate and bandwidth.

Our approach in this paper is to use a simple, but suboptimal technique for selecting redundant paths. In particular, we argue that finding two paths with absolute lowest loss rates for the proposed PDF system may not be needed in practice due to two reasons: (a) complexity increases due to active monitoring of probed packets and maintaining the link state information associated with all the paths i.e. scalability reasons, and (b) sending packets on two paths with the absolute lowest loss rates may not be necessary to achieve reasonable performance in a PDF system with appropriate FEC protection level. This can be justified considering the results in Section III, indicating that substantial gains can be achieved even in situations where the packet loss rate on the redundant path is many times that of the default path. Based on the above discussion, we propose a scalable, heuristic scheme to select the redundant path via a participating node using path information from traceroute tool. Traceroute can provide the names of the routers and roundtrip delays of links between the two communicating nodes on the Internet.

Let us formally denote a network topology as directed graph G = (V,E) consisting of the vertices vi ∈V and edges e = (vi,vj) ∈ E. Vertices vi's can be thought of as routers or domains, and the path p(v1,vn) = [v1,v2,...,vn] as the physical path from v1to vn. A redundant path p?(v1,vk,vn) from v1 to vn, via node vk is then p(v1,vk) ∪ p(vk,vn).

Associated with every pair of vertices (vi,vj) is a weight w(vi,vj). This weight can be thought of as delay, bandwidth, or loss rate associated with the physical link between vi and vj. Hence, the weight w(p(vk,vl)) associated with a path from vk to vl is the sum of the weights of the individual physical links joining vk and vl. In this paper, weights denote the latencies between participating nodes since they are readily available from traceroute. Let O = [vm,...,vn] be the set of participating nodes; then the relay node kj for creating the redundant path between vertices u and v is computed in a two-step procedure.

First, we compute a set of relay nodes Ot that result in the minimum number of joint links between the default Internet path and all the redundant paths via a node in O, namely, O^t= argmin k p^t(u,k,v) ∩ p*(u,v).

1. Where k ∈O, pt(u,k,v) denotes the redundant path via node k, and p*(u,v) denotes the default Internet path. Note that

the set O^t can have more than one element since there could potentially be two or more nodes in O that result in the same minimum number of joint links between the default and redundant paths. Since the average number of links between two nodes on the Internet the operation $p^t(u,k,v) \cap p^*(u,v)$ can be done fast. To find argmin k $p^t(u,k,v) \cap p^*(u,v)$, exhaustive search for the set of nodes O^t that results in minimum number of joint links between the redundant and default paths can be done in O(N) with N being the number of participating nodes.

2. Next, we choose the node k?that results in minimum weight associated with the corresponding redundant path, namely,

K^t= argmin l $w(p^t(u,l,v))$

where $l \in O^t$, Note that it is the sender that runs the redundant path selection algorithm, and that the input to the algorithm is the path information, specifically, the names of routers and the associated link latencies of the default path p(u,v) and the redundant paths $p^t(u,l,v)$. The names of the routers are used in the first step to compute the number of shared links between the redundant and default paths while the latencies are used in the second step to find the path with minimum delay. The link latencies and names of routers along the path p(u,v) are readily available using traceroute from node u to v. The latency and router information for redundant path $p^t(u,k,v)$ via node k can be obtained by executing traceroute twice, once from nodes u to k, and another time from nodes k to v. The information returned from the two traceroute executions is then concatenated to form the path p?(u,k,v). Note that sender either runs this algorithm at the beginning of the new session, or it can use the stored paths provided from previous session since the paths are relatively stable. This will reduce the overhead of executing traceroute unnecessarily.

Intuitively, the path selection scheme first finds a set of redundant paths that are as disjoint as possible from the default path. Within this set of redundant paths, it then selects the one that results in minimum latency. An alternative might seem to be to select the redundant path based on traffic characteristics of each link along the path between two nodes. However, since we do not have knowledge of loss rates and bandwidths for individual links, we choose the redundant path to be maximally disjoint with the default Internet path so as their losses are uncorrelated, this results in the PDF system to be effective in minimizing the packet loss rate.

V. Simulation Results

A. Simulation Topology

We use the Internet topology generator software Brit to generate various Albert-Barabasi topologies for all the simulations. Albert-Barabasi model has been shown to approximate the Internet topology reasonably well.

In particular, we generate two, two-level hierarchical Albert Barabasi models, and one flat Albert-Barabasi model. All topologies contain 1500 nodes each. The top level of the two-level hierarchical topology models the collection bottom level models the routers within an AS. The two two-level Albert-Barabasi models are meant to model wide area Internet topology consisting of many ASes with various degrees of interconnectivity, and the flat AlbertBarabasi model represents the router interconnectivity within an AS as shown in Figures 6 and 7, respectively . The relevant information for each simulated topology is listed in Table I. H-Albert-Barabasi stands for hierarchial Albert-Barabasi model.

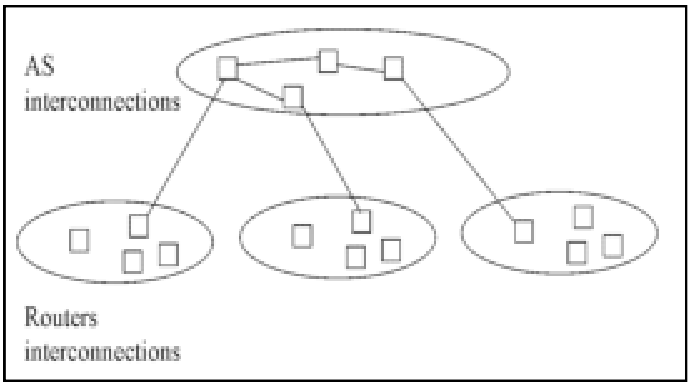


Fig. 6: Two Level Hierarchal Topology

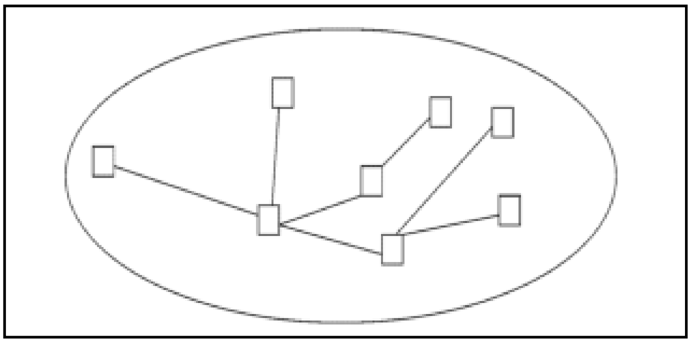
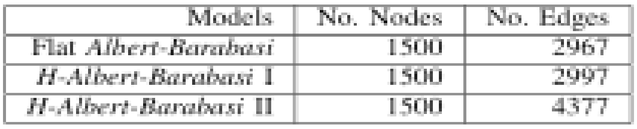


Fig. 7: Flat Topology

To estimate the average latency, hop counts, and the degree of disjointness between the redundant path and the default Internet path, we perform the following three steps in our simulations. In step one, we randomly choose a set of participating nodes. In step two, we randomly choose a pair of receiver and sender in the set of participating nodes. In step three, we use our scheme in Section V to find the redundant and the default paths for a given configuration of sender, receiver, and participating nodes. The default path in our simulations is assumed to be the one with smallest latency or equivalently the shortest path between the sender and receiver, and hence can be computed using OSPF algorithm for a given topology.

Table 1: Informations for Various Topologies



Models	No. Nodes	No. Edges
Flat *Albert-Barabasi*	1500	2967
H-Albert-Barabasi I	1500	2997
H-Albert-Barabasi II	1500	4377

This assumption is not critical to our redundant path selection scheme as we merely need a way to compute a default path. Next, we repeat step one to three over 5000 times to obtain the average latency, hop counts, and the number of shared links between redundant and default paths. Define the jointness percentage between the default and redundant paths as the number of shared links between them over the number of links of the default path. Figure 8 shows the jointness percentage between the default and redundant paths for all three topologies as a unction of percentage of participating nodes. As expected, the jointness percentage decreases as the number of participating nodes increases for all three topologies. This phenomenon is intuitively plausible since a redundant path is created via a participating node. Larger number of participating nodes allows more choices of redundant paths, thus producing more disjoint paths than a configuration with fewer participating nodes. As seen in Figure 7, on average, to achieve less than 10% shared links or less than one shared link between the default and redundant paths for all three topologies, only 2% of total nodes are required to be participating nodes. Another observation is that the percentage of shared links is smaller for Albert-Barabasi II model than that of Albert-Barabasi I. The reason is that Albert-Barabasi II has larger degree of interconnectivity between its nodes than that of Albert- Barabasi I; hence, more disjoint paths can be found. Note that the flat Albert-Barabasi model has the lowest ratio of all three topologies due to following reasons the top level of the two-level hierarchical AlbertBarabasi topologies represents interconnectivity between AS while the bottom level represents the interconnectivity between routers within an AS. If two participating nodes are located in two different ASes, all the paths between them must go through a few AS nodes. As a result, the redundant paths may share larger number of links with the default path than with a flat topology.

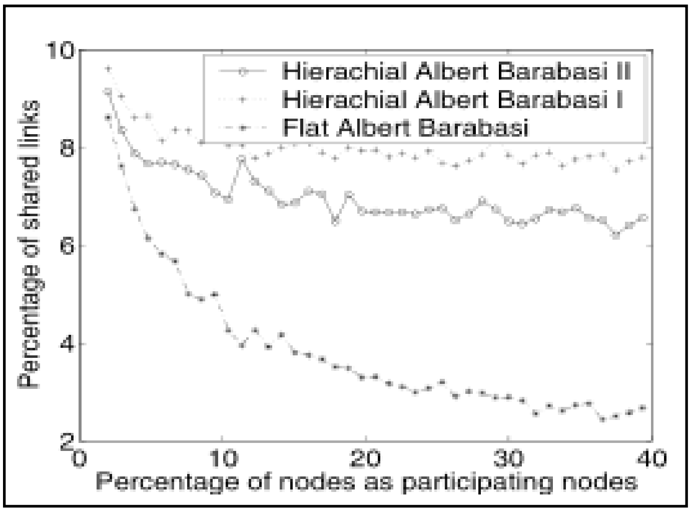


Fig 8: Percentage of Shared Link Between the Redundant Path and Default Path

For small percentage of participating nodes, the latency ratio of redundant over default paths is as high as 1.7. In this case, if the round-trip time of the default path is 100 milliseconds, then the average round-trip time of the corresponding redundant path is 170 milliseconds, thus exceeding the tolerable delay of 150 milliseconds for two-way interactive applications. This problem can be remedied by either increasing the percentage of participating nodes to 10%, or by allowing the redundant path to share larger number of links with the default path. With the default round-trip time of 100 milliseconds and with 10%, or more participating nodes, the average latency ratio of redundant over default paths is 1.5, corresponding to the delay of 150 milliseconds for the redundant path, thus satisfying the requirements for two-way interactive applications.

B. NS Simulation

In this section, we characterize the packet loss reductionfor various number of shared links between redundant anddefault paths using NS [16]. The simulation topology for the two disjoint redundant and default paths. Based on the average number of links between two participating nodes in Section VI-A, the number of links for default and redundant paths are set to 11 and 18 respectively. Each link's capacity is 2Mbs with propagation delay of 4 milliseconds. To simulate bursty packet loss of the Internet, random exponential traffic is generated at each link with the peak rate of 1.8Mbs, average idle period of 8 seconds, and the burst period of 40 milliseconds. We compare the packet loss rate for following three scenarios:

1. Sender streams the video to the receiver at 800kbps on the default path,
2. Sender streams the video to the receiver on both redundant and default paths at 400kbps for each path with two paths are assumed to be completely disjoint,
3. Same as scenario 2 except there is one shared link between redundant and default paths.

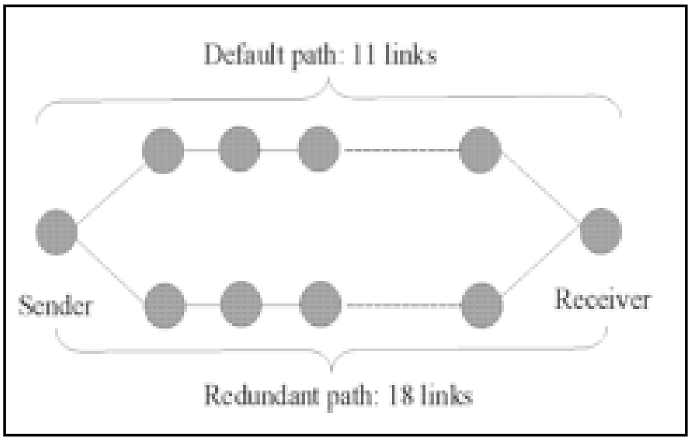


Fig 9: Simulation Configuration for Two Disjoint and Default Path

In all scenarios, the video packet size is 500 bytes, and packets are protected using Reed-Solomon code RS(30, 23) with 23 data packets and 7 redundant packets for each FEC block. Hence, if there are more than 7 lost packets per FEC block, then lost packets cannot be entirely recovered. Fig. 12, 13, and 14 show the number of lost packets per 30 packets versus the packet sequence number for scenarios 1, 2, and 3, respectively. The points above the horizontal line represent irrecoverable loss events. As seen, there are considerably more irrecoverable loss events for scenario 1 than for 2. This is intuitively plausible since sending packets at a lower rate on multiple independent paths transforms the bursty loss behavior of a single path into a uniform loss behavior, thus reducing the burstiness, and increasing the recoverable probability. Also, the number of irrecoverable loss events for scenario 3 is larger than that of 2. This is due to the one shared link between the redundant and default paths in scenario 3. Assuming that links are independently congested, the larger number of shared links between the redundant and default paths leads to higher chance of simultaneous bursty loss on both paths, for which FEC is ineffective. One can think of scenario 1 where all packets are sent on only default path as an extreme case of path diversity in which all the links of two paths are shared.

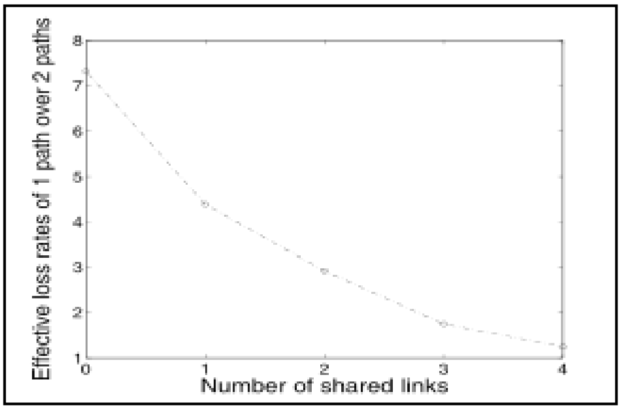


Fig. 10: Ratio of Average Loss Rate

The recoverable probability of FEC decreases as the number of shared links between the redundant and default paths increases. To characterize the effect of number of shared links on the loss rate, the ratio of the effective packet loss rate of uni-path scheme to that of dual path scheme as a function of number of shared links between them. The effective packet loss rate is the ratio between the number of irrecoverable lost packets and the total sent packets. As seen, the effective loss rate for the single path scheme is more than 7 times that of the path diversity scheme with completely disjoint redundant and default paths. The reduction in effective loss rate from using path diversity decreases as the number of shared links between the two paths increases. However, even when 3 of out 11 links are shared, the effective loss rate using path diversity scheme is twice smaller than that of using unipath scheme.

VI. Conclusion

We have proposed a PDF system for delay sensitive applications over packet switched networks along with the Nymble a comprehensive credential system called Nymble, which can be used to add a layer of accountability to any publicly known anonymizing network. Servers can blacklist misbehaving users while maintaining their privacy, and we show how these properties can be attained in a way that is practical, efficient, and sensitive to needs of both users and services in which when error occurs, the disjoint paths from a sender to a receiver are established using a collection of relay nodes. A scalable, heuristic scheme for selecting a redundant path has been proposed, and the resulting redundant path's lengths and disjointess for various Internet like topologies have been characterized. Our simulations have demonstrated that, for various Internet-like topologies, only 10% of participating nodes are required for the proposed path redundant selection scheme to effectively find a redundant path sharing 2 or fewer links with the default path; this effectively results in a factor of 3 reduction in irrecoverable packet loss as compared to uni-path scheme.

VII. Future Enhancement

It is an open source we can continue of approach for better results with the Puzzle based defense strategy against the attackers.

Refrences

[1] W. Tan, A. Zakhor,"Real-time internet video using error resilient scalable compression and tcp-friendly transport protocol", IEEE Trans- actions on Multimedia, Vol. 1, pp. 172–186, june 1999.

[2] G. De Los Reyes, A. Reibman, S. Chang, J. Chuang, "Error-resilient transcoding for video over wireless channels", IEEE Transactions on Multimedia, Vol. 18, pp. 1063–1074, june 2000.

[3] J. Robinson, Y. Shu,"Zerotree pattern coding of motion picture residues for error-resilient transmission of video sequences", IEEE Journal on Selected Areas in Communications, Vol. 18, pp. 1099–1110, June 2000.

[4] H. Ma, M. Zarki,"Broadcast/multicast mpeg-2 video over wireless channels using header redundancy fec strategies", in Proceedings of The International Society for Optical Engineering, November 1998, Vol. 3528, pp. 69–80.

[5] W. Tan, A. Zakhor,"Error control for video multicast using hierarchical fec", in Proceedings of 6th International Conference on Image Processing, October 1999, Vol. 1, pp. 401–405.

[6] G. Ateniese, J. Camenisch, M. Joye, G. Tsudik.,"A Practical and Provably Secure Coalition-Resistant Group Signature Scheme", In CRYPTO, LNCS 1880, pp. 255-270. Springer, 2000.

[7] G. Ateniese, D. X. Song, G. Tsudik,"Quasi-Efficient Revocation in Group Signatures", In Financial Cryptography, LNCS 2357, pp. 183-197. Springer, 2002.

[8] M. Bellare, R. Canetti, H. Krawczyk,"Keying Hash Functions for Message Authentication", In CRYPTO, LNCS 1109, pp. 1-15. Springer, 1996.

[9] M. Bellare, A. Desai, E. Jokipii, P. Rogaway,"A Concrete Security Treatment of Symmetric Encryption", In FOCS, pp. 394-403, 1997.

[10] M. Bellare, P. Rogaway,"Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols", In Proceedings of the 1st ACM conference on Computer and communications security, pp. 62-73. ACM Press, 1993.

[11] M. Bellare, H. Shi, C. Zhang,"Foundations of Group Signatures: The Case of Dynamic Groups", In CT-RSA, LNCS 3376, pp. 136-153. Springer, 2005.

[12] D. Boneh, H. Shacham,"Group Signatures with Verifier-Local Revocation", In ACM Conference on Computer and Communications Security, pp. 168-177. ACM, 2004.

[13] S. Brands,"Untraceable Off-line Cash in Wallets with Observers (Extended Abstract)", In CRYPTO, LNCS 773, pp. 302-318. Springer, 1993.

A.Thirupathaiah, received M.tech(IT) from Punjabi University in Nov 2003,Patiala.He worked as a Assoc. Professor in St.Anns college of engineering & Technology, in the period of (2008-2010).He is currently pursuing M.tech in computer science & engineering at St.Anns college of Engg. & technology which is affiliated under the JNTU, Kakinada. He is member of CSI and MISTE .He has total of 11 years of experience in Teaching field. He is a Life time Member of ISTE and CSI. His area of interests are Computer Networks , Network Security and Cloud Computing.

K.Eswar received the B.tech from Bapatla engineering college in computer science & engineering in 2002. He received his M.tech from Andhra university in computer science & engineering in 2004.Currently, He is working as a Assoc.Prof, in St.Anns college of engineering & Technology which is affiliated under JNTU Kakinada which is permanent NBA accreated Institue. He is member of CSI .He has total of 10 years of experience. His research interest includes Data Mining, Cloud omputing, Computer Architecture and .He is a Sr. member of ISTE, SIEEE.

Dr.P.Harini received B.E. degree in Electronics and Communications Engg. form University of Madras, Chennai, in1993, received M.Tech. degree in Remote Sensing from JNTU, Hyderabad, in 1997, received M.Tech. degree in Computer Science and Engineering from JNTU, Hyderabad,in 2003 and received Ph.D. in Computer Science and Engineering from JNTU, Anantapur, in 2011. She has 16 Years of Experience in which 1 year of Industrial, 1 year of Research & over 14 years of rich Teaching Experience in reputed Engineering Colleges & She is currently working as Professor & HOD in Computer Science & Engineering department in St.Ann's College of Engineering & Technology, Chirala. She Published 21 Research papers in various International Journals & Conferences. Guided many UG & PG students for projects & Life time Member of ISTE & CSI. Conducted successfully many Workshops, Seminars, conferences, FDPs and many National Level Technical Symposiums.