Adaptive and iterative multipath routing mechanism for High Speed Networks

Sunil Kumar
Shobhit University,
Meerut, U.P., INDIA.
(mtechsunilarora@gmail.com)

A. K. Vatsa
Shobhit University
Meerut, U.P., INDIA.
avimanyou@rediffmail.com

Abstract- The advances in computing and networking technology due to transmission of bulk amount of data in various services like multimedia data communication. There is need of high speed network and therefore at the network level, the route selection and resource reservation are the major issues due to fluctuations in traffic load, link failures and topology changes. The routing mechanism may provide the optimal route in the hierarchical network environment from the perspectives of maximization of network resource utilization. Therefore, in this paper, we proposed an Adaptive and iterative multipath routing mechanism and the architecture to search the multiple paths from the source to destination.

Keywords: Routing algorithm, High-speed networks, Hierarchical, ATM, ISDN, Competitive Routing and Multipath Routing.

I. Introduction

Recent years have seen great advances in computing and networking technology. At the network level, new high-speed technologies such as Asynchronous Transfer Mode (ATM), Integrated Service Digital Network (ISDN), Digital Subscriber Line (DSL) and Fiber Distributed Data Interface (FDDI) networks are actively being deployed in research institutions and industry [17]. These networks not only have the capability of transmitting information at high speed, but also have the potential to offer a wide range of Quality of Service (QoS) properties including bounds on delay, guarantees on throughput and isochronous communications. The accelerating demand for remote data access, web services, great computing capabilities regardless of user location and mobility require a communication infrastructure with higher and more bandwidth.

Broadband offers a new brand of services where data, voice, and video commonly known as multimedia can be delivered together as one packet. Broadband is often called "high-speed" access to the Internet, because it usually has a high rate of data transmission [25]. In general, any connection to the customer of 256 kbit/s or greater is more concisely considered broadband Internet access. Some of the networks that are available for providing these types of services are Asynchronous Transfer Mode (ATM), frame relay, and leased lines.

As Broadband Integrated Services Digital Networks (B-ISDN) standards and high-speed networks emerge, modern networks are expected to provide a wide range of services [3]. Routing is the process of selecting paths in a network along which to send network traffic. Routing is performed for many kinds of networks, including the telephone network (Circuit switching), electronic data networks (such as the Internet), and transportation networks. Path selection in network routing has typically been formulated as a shortest path problem. There is also the problem of routing in a dynamic environment due to fluctuations in traffic load, link failures and topology changes[2]. Hierarchical network deployment is one of the popular approaches for providing network scalability, such as PNNI [ATM96b] and OSPF [MOY94]. It is based on network topology abstraction and decomposition of large-scale networks from the perspective of the management domain [1].

Multipath routing schemes distribute traffic among multiple paths instead of routing all the traffic along a single path. Two key questions that arise in multipath routing are how many paths are needed and how to select these paths. Multipath routing has been extensively studied and used in all kinds of existing communication networks like the Internet, high speed networks and ATM networks based on the QoS requirements [14]. In a single-path routing infrastructure, only a single path exists between any two networks in the internetwork. While this may simplify the routing tables and the packet flow paths, single-path internetworks are not fault tolerant. A fault can be sensed with a dynamic router, but the networks across the failure are unreachable for the duration of the fault. A downed link or a downed router must be brought back up before packets can be delivered successfully across the downed link or router [24].

In a multipath routing infrastructure, multiple paths exist between networks in the internetwork. Multipath internetworks are fault tolerant when dynamic routing is used, and some routing protocols, such as OSPF, can balance the load of network traffic across multiple paths with the same metric value. Multipath internetworks, however, can be more complex to configure and can have a higher probability of routing loops during convergence when using distance vector–based routing protocols [24].

Adaptive routing algorithms in contrast change their routing decisions to reflect changes in the topology, and usually the traffic as well. Adaptive algorithm differs in where they get their information (e.g. locally from adjacent routers, or from all routers), when they change the routes, and what metric is used for optimization (e.g. distance, number of hops, or estimated transit time). It has low routing overhead.

The iterative routing, the source try to find a sequence of nodes to which other intermediate nodes have to just iterate or multi-pass thoroughly until the destination is reached.

At the network level, the route selection and resource reservation are the major issues in high speed network due to fluctuations in traffic load, link failures and topology changes[21-22]. The routing mechanism may provide the optimal route in the hierarchical network environment from the perspectives of maximization of network resource utilization.

Paper Organisation- The organization of this paper is as follows. The introductory part discussed in Section-1 under head of Introduction. The paper reviews part has been described in Section-2 under the head of Backgrounds. The proposed routing mechanism and architecture has been illustrated in Section-3 under the head of Proposed Work. The Data Transfer mechanism has been described in Section-4 under the head of Data Transfer mechanism. The conclusion and future scope of this paper has been discussed in Section-5 and Section-6 respectively.
II. Backgrounds

For the multi-constrained routing problem a heuristic algorithm\[4\], which involves two or more additive weight functions, has been proposed. In the case of delay-cost routing, the algorithm first maps the costs to bounded integers and then uses an extended Dijkstra’s algorithm to find a solution for the new problem. A feasible path of the new problem is shown to be also a feasible path of the original problem.

For services with delay guarantees \[5-6\] showed that when a broad class of WFQ-like scheduling algorithms are used, the bandwidth, delay, jitter and/or buffer space bounds are not independent. Finding a path that satisfies delay, jitter, and buffer space constraints is solvable in polynomial time only if the relationship between bandwidth, delay and jitter is taken into consideration.

A framework for online throughput competitive routing \[7-8\] has been proposed. This algorithm combines routing and admission control into a single strategy. It assigns each link a length which is an exponential function of the current bandwidth utilization on the link. If no sufficiently short path exists, the request will be rejected. A competitive ratio is defined to compare the performance achieved by the online routing algorithm over the performance achieved by the optimum offline routing algorithm with all the input sequences, and the performance of the algorithm is measured in terms of a bandwidth-duration product, i.e. the throughput.

The Wang-Crowcroft algorithm \[9-10\] finds a path for any given constraint on bottleneck bandwidth and propagation delay. First, any link with a bandwidth less than the requirement is eliminated so that any path in the resulting network topology graph satisfies the bandwidth constraint. Then the path with minimum length is computed using Dijkstra’s algorithm to determine whether a feasible path exists. They also proposed two distributed algorithms for hop-by-hop routing.

A call-by-call source routing strategy\[11\] that makes use of rule based fallbacks. This strategy provides a flexible platform on which routing can be done efficiently subject to performance, resource and priority constraints. The fallback routing algorithm sequentially computes paths based on a predetermined fallback sequence of routing instances, until an acceptable one is available or the call will be blocked. The proposed routing architecture uses hierarchical source routing with optional crankbacks. A variety of traffic-dependent QoS-related topology state parameters are advertised to support call-level QoS matching. Topology information at each hierarchical level is aggregated to trade-off fine-grain QoS matching for scalability in very large networks.

A new QoS routing algorithm\[12\] for ATM networks which is compliant with the PNNI protocol has been proposed. The algorithm tries to find a path iteratively with different sets of path search approaches until the obtained path meets the requested QoS. The procedure is as follows: First, a candidate path that satisfies the QoS requirements is found. The algorithm then prunes all links that cannot guarantee the requested bandwidth from the whole known topology information, by calculating the equivalent bandwidth of the requested call and comparing it with the available bandwidth for each link. From this reduced set, one or more possible paths are chosen.

The distributed algorithms for the secure multipath routing\[23\] has been explained. In this routing, data sent on the multipath so that intruders require much more resources to mount successful attacks. The paper includes (1) distributed routing decisions (2) bandwidth- constraint adaptation (3) lexicographic protection. In the paper two algorithms are used for the solution (1) Bound control algorithm (2) Lex control algorithm and prove their convergence to the respective optimal solution. The basic of paper is to design a distributed solution, which implement the selecting data across the multipath on the architecture.

III. Proposed Work

The proposed mechanism for an adaptive and iterative multipath routing for High speed network. The proposed architecture and mechanism is discussed in Section 3.1 and 3.2 respectively.

**Proposed Architecture**

The proposed architecture provides the optimal routing service in a hierarchical based high speed network with routing scheme. This architecture is comprised of three components: 1. Network Topology and route info. Manager(NwMgr), 2. Fault Manager (FaultMgr) and 3.Route Manager(RouteMgr).

*Figure 1: Adaptive and iterative Multipath Routing Architecture.*
The NwMgr first, assigns the node address and link state attributes and metric parameters, then the node initiator assemble all the state information into an ‘Initiate’ packet and send to its neighbour nodes. In the DB Sync. Process, nodes updates its topology database with HTSEs(Hierarchal Topology State Element). In the flooding process, A node in the peer group proceeds to propagate the topology information to all members of the group. Receiving node send the acknowledgement to the receipt, then all the nodes update its topology database.

In the Info. Flow Process, the Group Leader summarizes the topology info. of all nodes of its peer group and propagates the info. to its upper level Group. Address summarization, to represent a collection of end systems by the single reachable address prefix, is performed.

Topology aggregation process of reducing topology information by summarizing nodal as well as link information, is performed. All the summerized topology information is passed to the RouteMgr.

The RouteMgr perform the adaptive path search algorithm and maintain the searched path in RouteStack and provide the acknowledgement when the destination node is found.

The FaultMgr perform the crankback process, when the path not reachable or the selected path contains a bottleneck node/link. It provides the alternate path to the route manager for the same destination node.

3.2 Proposed Mechanism

Phase - I: Network Topology, Context and state Acquisition

Step – 1: Network Topology and State Parameters

NetworkTopologyContextAcquisition( )

{ 
  * AssignNode’s _address( )
    
    Assign a unique address dynamically using the DHCP server.
  
  * FindNetworkTopology_State( )
    
    //Link State Attribute parameters are Available Cell Rate (ACR), Max. Cell Rate(MaxCR), Cell Rate Margin(CRM), Variance Factor(VF).
    * Assign the values to the link state attributes.
    
    // Metric Parameters such as cell transfer delay (CTD), jitter or Cell Delay Variation (CDV) and cell loss ratio (CLR), Administrative weight(AW)
    * Assign the values to the Link State Metric parameters.

  }

Step – 2: 
RouteInfoFlow_Computation ( )

{ 
  If (Node is Active)
  
  Node_Initilization( );
  Database_Synchronization ( );
  Flooding( );
  Info_Flows ()
  AddressSummarizations_Topology Aggregation();

  }

Node_Initilization ( )

{ 
  * Packet Initialization Data(PID) assemble all the state information into an ‘Initiate’ packet( End-system address, Node ID, Hierarchal Group ID[HGID]).
  * Send ‘Initiate’ packet to its immediate neighbours.
  * Neighbour compare the received HGID with its own HGID.
  * If both match, node tries to synchronize its topology database.

  }

Database_Synchroniztion ( )

{ 
  * HTSE Header (HTSE ID, sequence number, checksum, remaining lifetime) is created .
  * Nodes Exchange the Hierarchal Topology State Element (HTSE) header information.
  * Node requests for the advertised HTSE.
  * Node updates its topology database with received HTSE.

  }

Flooding()

{ 
  * A node in the peer group proceeds to propagate the topology information to all members of the group.
  * HTSEs are bundled within a Hierarchal Topology State Packet (HTSP) and transmitted to all the neighbouring nodes.
  * Receiving node send the acknowledgement to the receipt.
  * Node update its topology database.

  }

Info_Flows()

{ 
  * Group Leader summarizes the topology info. of all nodes of its peer group e.g GL(X,Y)
  * Group leader propagates the info. to its upper level Group e.g. GL(X).
  * Other side, a GL receives downward info. of the same higher-level group.
  * The GL then propagate the received info. to all members of the group.

  }

AddressSummarizations_Topology Aggregation()

{ 
  * Address summarization, a process of the single reachable address prefix to represent a collection of end systems, is performed.
  * Process of reducing topology information by summarizing nodal as well as link information, is performed.
  * Helps in hiding the internals of a group as well as reduce the flow of control in the network.
  * Makes maintenance of topology information easier.

  }

Phase II: Route Selection Process

AdaptivePathSearch()

{ 
  //Every route maintain the following information.
  Bandwidth(BW) of route, Cell Delay Variation(CDV),
The proposed routing mechanism is effective and efficient for high speed networks but it does not guarantee the delivery of packets under situations where non-uniform transmission ranges exist and to improve the algorithm to include the integration of link utilization as well as security of the link and data over multiple paths.

V. Conclusion

In this paper, the proposed adaptive and iterative multipath routing architecture and mechanism for High speed networks is effective and efficient and it takes advantage of the PNNI hierarchical structure to reduce path computation complexity and maximize network throughput. It would works in very effective and efficient manner over the high speed network. But the heterogeneous nature of node, someone affects it’s effectiveness particularly when network scalability feature is very high, although, at low scalability it would be very efficient. As in the era of communication particularly, when communicating nodes changes their locations then it’s efficiency is get reduced.

VI. Future Scope

The proposed routing mechanism is effective and efficient for high speed network but it does not guarantee the delivery of packets under situations where non-uniform transmission ranges exist and to improve the algorithm to include the integration of link utilization as well as security of the link and data over multiple paths.
References


23. Patrick C.C. Lee, Vishal Misra and Ruben Stein, “Distributed algorithm for secure multipath routing”, International symposium on circuits and system,
Author Profile

Avimanyou K. Vatsa is working as Assistant Professor at Shobhit University, Meerut, (U.P.), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech(I.T.) from V.B.S. Purvanchal University, Jaunpur (U.P.). He has worked as software engineer in software industry. He has been in teaching from more than one decade. During this short period of time, he has supervised more than 25 dissertation of M.Tech. students. He is on the editorial board of few international journals in network and security area. He has been member of several academic and administrative bodies. During his teaching he has coordinated several Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national and international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).

Sunil Kumar is working as Assistant Professor at IMT Group of Colleges, Meerut (U.P.). He obtained his M-Tech (Computer Engineering) from Shobhit University and MCA from RVD University, Udaipur (Rajasthan) and ‘A’ Level Certificate from DOEACC Society, New Delhi. He has been in teaching since Five years. During his teaching he has coordinated several Technical fests and National Conferences at Institute level. He has attended several seminars, workshops and conferences at various levels. His area of research includes High Speed Networks, MANET (Mobile Ad-Hoc network), Cloud Computing and Network Security.