

# **2009 -10 IEEE PAPERS**

## **Titles & Abstracts For M-Tech**

1. ONLINE INDEX RECOMMENDATIONS FOR HIGH-DIMENSIONAL DATABASES USING QUERY WORKLOADS
2. QUIVER: CONSISTENT OBJECT SHARING FOR EDGE SERVICES
3. HYBRID SCHEDULING OF DYNAMIC TASK GRAPHS WITH SELECTIVE DUPLICATION FOR MULTIPROCESSORS UNDER MEMORY AND TIME CONSTRAINTS
4. RATE AND DELAY GUARANTEES PROVIDED BY CLOS PACKET SWITCHES WITH LOAD BALANCING
5. TWO TECHNIQUES FOR FAST COMPUTATION OF CONSTRAINED SHORTEST PATHS
6. MEASUREMENT-BASED ADMISSION CONTROL AT EDGE ROUTERS
7. DESIGNING LESS-STRUCTURED P2P SYSTEMS FOR THE EXPECTED HIGH CHURN
8. C-TREND: TEMPORAL CLUSTER GRAPHS FOR IDENTIFYING AND VISUALIZING TRENDS IN MULTIATTRIBUTE TRANSACTIONAL DATA
9. CONTROLLING IP SPOOFING THROUGH INTERDOMAIN PACKET FILTERS
10. USING THE CONCEPTUAL COHESION OF CLASSES FOR FAULT PREDICTION IN OBJECT-ORIENTED SYSTEMS
11. MITIGATING PERFORMANCE DEGRADATION IN CONGESTED SENSOR NETWORK
12. LOCATION-BASED SPATIAL QUERY PROCESSING IN WIRELESS BROADCAST ENVIRONMENTS
13. INTRUSION DETECTION IN HOMOGENEOUS AND HETEROGENEOUS WIRELESS SENSOR NETWORKS
14. A PRIORITY BASED MAC SCHEDULING ALGORITHM FOR ENHANCING QOS SUPPORT IN BLUETOOTH PICONET
15. TCP-LP; LOW PRIORITY SERVICE VIA END POINT CONGESTION CONTROL
16. DISTRIBUTED & COLLABORATIVE KEY AGREEMENT PROTOCOLS WITH AUTHENTICATION & IMPLEMENTATION FOR DYNAMIC PEER GROUPS.
17. PROVABLY SECURE 3 PARTY AUTHENTICATED QUANTUM KEY DISTRIBUTION PROTOCOL
18. A DISTRIBUTED DATABASE ARCHITECTURE FOR GLOBAL ROAMING IN NEXT -GENERATION MOBILE NETWORKS.
19. MINIMIZING FILE DOWNLOAD TIME IN STOCHASTIC PEER-TO-PEER NETWORKS
20. FACE RECOGNITION SYSTEM
21. DISTRIBUTED CACHE ARCHITECTURE WITH SNOOPING FOR QOS ROUTING IN LARGE NETWORKS
22. ONLINE HANDWRITTEN SCRIPT RECOGNITION
23. IMAGE DOWNLOADING RANGE PERFORMANCE EVALUATION OF JAVA-REMOTE METHOD INVOCATION.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalsolutions.com](mailto:raghav@goalsolutions.com)



24. HYBRID INTRUSION DETECTION WITH WEIGHTED SIGNATURE GENERATION OVER ANOMALOUS INTERNET EPISODES
25. A HIERARCHICAL MODELLING AND ANALYSIS FOR GRID SERVICE RELIABILITY
26. SLA-DRIVEN CLUSTERING OF QOS AWARE APPLICATION SERVERS.
27. HIDING SENSITIVE ASSOCIATION RULES WITH LIMITED SIDE EFFECTS
28. CRYPTOGRAPHIC VERSUS TRUST-BASED METHOD FOR MANET ROUTING SECURITY
29. AN EFFICIENT CLUSTERING SCHEME TO EXPLOIT HIERARCHICAL DATA IN NETWORK TRAFFIC ANALYSIS
30. PROBLEM ORIENTED SOFTWARE ENGINEERING: SOLVING THE PACKAGE ROUTER CONTROL PROBLEM
31. A SECURE MANET ROUTING PROTOCOL FOR DETECTING FAULTY LINKS.
32. PC REMOTE
33. LOAD BALANCING IN DISTRIBUTED VOD USING LOCAL PROXY SERVER GROUP[LPSG TRACKER]
34. CREDENTIAL CENTER
35. PRE ACTIVE CIRCULATED CACHE UPDATING USING ON DEMAND ROUTING PROTOCOL
36. DYNAMIC SOURCE ROUTING USING LOCATION AIDED ROUTING PROTOCOL
37. EFFECTIVE PACKET ANALYZING & FILTERING SYSTEM FOR ATM NETWORKS
38. DYNAMIC SEARCH ALGORITHM IN UNSTRUCTURED PEER TO PEER
39. DATA MANAGEMENT SYSTEM USING PROXIES
40. PROBABILISTIC PACKET MARKING FOR LARGE SCALE IP TRACE BACK
41. EVALUATION OF MIDDLE WARE ARCHITECTURE FOR ENABLING SERVICE LEVEL AGREEMENT APPLICATION SERVERS
42. EFFICIENT KEY MANAGEMENT FOR THRESHOLD MULTISIGNATURE IN DISTRIBUTED SYSTEMS
43. INTRUDER DETECTION SYSTEM OVER ABNORMAL INTERNET SEQUENCE
44. THE PLAGIARISM HUNTER
45. TRUTH FINDER ON THE WEB \*\*A
46. IDENTITY BASED CRYPTOGRAPHY IN EMAIL APPLICATION \*
47. HANDLING NAT TRAVERSAL PROBLEM ON SECURITY OF VOIP
48. GLOBAL WEB RATING
49. ROUTE INFORMATION SYSTEM FOR CHENNAI
50. GIFT GIVING APPROACH IN FILE SHARING NETWORK
51. A SIGNATURE BASED INDEXING METHOD FOR EFFICIENT CONTENT BASED RETRIEVAL OF RELATIVE DATA
52. MANY MORE.....

#### TECHNICAL REQUIREMENTS

- CORE JAVA
- SWINGS
- NETWORKING
- J2EE
- JSP
- EJB

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



- STRUTS

## 1 . Online Index Recommendations for High-Dimensional Databases Using Query Workloads

**Scope of the project:**In this project we are going to develop one index for High Dimensional database using user query pattern , by this index we can able to retrieve the data faster, and we make this index adjust itself when the user query pattern change.

**Introduction:**AN increasing number of database applications such as business data warehouses and scientific data repositories deal with high-dimensional data sets. As the number of dimensions/attributes and the overall size of data sets increase, it becomes essential to efficiently retrieve specific queried data from the database in order to effectively utilize the database. Indexing support is needed to effectively prune out significant portions of the data set that are not relevant for the queries.

**Modules:**

- Initialize the abstract Representation
- Calculate the Query Cost
- Select Best Indexes
- Calculate the performance

## 2. Quiver: Consistent Object Sharing for Edge Services

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Abstract** We present Quiver, a system that coordinates service proxies placed at the "edge" of the Internet to serve distributed clients accessing a service involving mutable objects. Quiver enables these proxies to perform consistent accesses to shared objects by migrating the objects to proxies performing operations on those objects. These migrations dramatically improve performance when operations involving an object exhibit geographic locality, since migrating this object into the vicinity of proxies hosting these operations will benefit all such operations. This system reduces the workload in the server. It performs the all operations in the proxies itself. In this system the operations performed in First-In-First-Out process. This system handles two process serializability and strict serializability for durability in the consistent object sharing. Other workloads benefit from Quiver, dispersing the computation load across the proxies and saving the costs of sending operation parameters over the wide area when these are large. Quiver also supports optimizations for single-object reads that do not involve migrating the object. We detail the protocols for implementing object operations and for accommodating the addition, involuntary disconnection, and voluntary departure of proxies. Finally, we discuss the use of Quiver to build an e-commerce application and a distributed network traffic modeling service.

**Existing System:**

- In the existing system the proxies has been maintained in the critical path for each object updation or each proxy should connected with the centralized server.
- The consistency was not maintained while sharing the object.
- If the proxy has failed means the object has been lost.
- The existing system supports only single-object operations, and provides weak consistency semantics.

**Disadvantages:**

- Consistency was not maintained while migrating the object between the proxies.
- It does not handle the proxy disconnections.
- It supports only the single object operations.

**Proposed System:**

- This system forms the proxies in the tree structure. It shares the objects within the proxies. It reduces the workload in the server.
- Quiver enables consistent multiobject operations and optimizations for single-object reads that are not possible in these prior algorithms.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



- This system recovers the proxy disconnection. The disconnected proxies maintained by alternate proxies or it will be maintained through server.
- This System use the kruskal's algorithm for maintaining tree structure. It reduces weightage in the tree structure.
- It holds the object even when the proxy has been disconnected.

### 3. Hybrid Scheduling of Dynamic Task Graphs with Selective Duplication for Multiprocessors under Memory and Time Constraints

**Scope** This project deals with the processors execution time. Based on the execution time performance will be evaluated.

**ABSTRACT** MULTIPROCESSOR-BASED embedded systems have become quite widespread in recent times. Embedded systems such as personal handheld devices, set-top boxes, and miniprinters consist of complex applications with real-time Performance requirements. For such applications, a multiprocessor architecture is getting increasingly preferred over a single processor solution to achieve the required performance. Each processor in a multiprocessor system usually has its local memory for code storage and execution.

#### Modules

- Static Mapping
- Selective Duplication
- Online Scheduling

#### Advantages

- The execution time will be lesser, so the performance of the processor will be high.
- Multiprocessor is used to get a required performance over a single processor system.

#### Applications

- It is used, where the processor based system is running.
- Mainly it was used in embedded system applications.

### 4. Rate and Delay Guarantees Provided by Clos Packet Switches with Load Balancing

#### Scope of the project:

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



In this project we are going to increasing the data flow rate and at the same time we are going to reducing the delay while transferring the packets by using Clos packet switches. From this architecture we are getting higher transfer rate over the medium.

### Introduction

THE CLOS circuit switch has been proposed by Clos in 1953s at Bell Labs. This interconnection rule is: the xth SE in some switching stage is connected to the xth input of each SE in the next stage [6]–[8]. Here, all connections have the same bandwidths. It has been shown that a circuit can be established through the Clos switching fabric without rearranging existing circuits as long as the number of SEs in the second stage is at least twice the number of inputs of an SE in the first stage minus 1, i.e., . It has also been shown that a circuit can be established through the Clos switching fabric as long as the number of SEs in the second stage is no less than the number of inputs of an SE in the first stage, i.e., . In the latter case, the number of required SEs and their total capacity are smaller due to the fact that the existing circuits can be rearranged. While the complexity of the switching fabric hardware is reduced, the complexity of the algorithm for a circuit setup is increased. In both cases, non-blocking property of the Clos architecture has been proven assuming the specific algorithms for circuit setup [8]. Various implications of Clos findings have been examined in [12].

### Modules

- Packet Creation
- Forwarded Input to Centralized Switch
- Load Balancing
- Forwarded to Centralized Switch to Output Switch

## 5. Two techniques for fast computation of constrained shortest paths >>>>>Analysis phase...

## 6. Measurement based admission control at edge routers

**Abstract:** It is very important to allocate and manage resources for multimedia traffic flows with real-time performance requirements in order to guarantee quality of service (QoS). In this paper, we develop a scalable architecture and an algorithm for admission control of real-time flows. Since individual management of each traffic flow on each transit router can cause a fundamental scalability problem in both data and control planes, we consider that each flow is classified at the ingress router and data traffic is aggregated according to the class inside the core network as in a DiffServ

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



framework. In our approach, admission decision is made for each flow at the edge (ingress) routers, but it is scalable because per-flow states are not maintained and the admission algorithm is simple. In the proposed admission control scheme, an admissible bandwidth, which is defined as the maximum rate of a flow that can be accommodated additionally while satisfying the delay performance requirements for both existing and new flows, is calculated based on the available bandwidth measured by edge routers. The admissible bandwidth is a threshold for admission control, and thus, it is very important to accurately estimate the admissible bandwidth. The performance of the proposed algorithm is evaluated by taking a set of simulation experiments using bursty traffic flows.

### Existing System

- Existing schemes do not consider a long-range dependence property which is an important characteristic of the current internet traffic
- if we calculate the effective bandwidth just based on the parameters of long-range dependent traffic considering some QoS  
Such as loss probability, the utilization of the bandwidth can be very low due to huge rate fluctuation

### Proposed System:

- In the proposed scheme, admission decision is made for each Flow at the ingress routers, but it is scalable because per-flow States are not managed and the admission algorithm is simple.
- An ingress router manages the admissible bandwidth, which is a threshold for admission control, for each relevant egress router.
- Since the admissible bandwidth is calculated considering the delay QoS, it is possible to guarantee the delay performance by the proposed admission control scheme.

## 7. Designing Less-Structured P2P Systems for the Expected High Churn

**INTRODUCTION** PEER-TO-PEER (P2P) computing can be defined as the sharing of computer resources and services by direct exchange between the participating nodes. Since Napster's introduction in the late 1990s, the area has received increasing attention from the research community and the general public. Peers in P2P systems

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



typically define an overlay network topology by keeping a number of connections to other peers, their “friends,” and implementing a maintenance protocol that continuously repairs the overlay as new members join and others leave the system.

Due in part to the autonomous nature of peers, their mutual dependency, and their astoundingly large populations, the transience of peers (a.k.a. Churn) and its implications on the overall system’s performance have recently attracted the attention of the research community. A well-accepted metric of Churn is *node session time*—the time from the node’s joining to its subsequent leaving from the system.<sup>1</sup> Measurement studies of deployed P2P systems have reported *median session times* varying from one hour to one minute

The implications of such degrees of Churn on the system’s performance are directly related to the degree of peers’ investment in their friends. At the very least, the amount of maintenance-related messages processed by any node would be a function of the degree of stability of the node’s neighboring set. Beyond this, and in the context of content distribution P2P systems, the degree of replication, the effectiveness of caches, and the spread and satisfaction level of queries will all be affected by how dynamic the peers’ population is.

Our work addresses the problem of highly transient@□□□ulations in unstructured and loosely-structured P2P systems (collectively, *less-structured P2P systems*). Through active probing of over half a million peers in a widely deployed P2P system, we determined that the session time of peers can be well modeled by a Pareto distribution. In this context, the implication is that the expected remaining session time of a peer is directly proportional to the session’s current length, i.e., the peer’s age. This observation forms the basis for a new set of protocols for peer organization and query-related strategies that, by taking into consideration the expected session times of peers, yield systems with performance characteristics that are more resilient to the natural instability of their environments. We do this using a set of illustrative organizational protocols combined with a number of currently adopted and proposed query-related strategies, including methods for query distribution, caching and replication.

### Modules

- Peer Request
- Superpeer Response
- Upload
- Superpeer updating
- File request
- Response

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



## 8. C-TREND: Temporal Cluster Graphs for Identifying and Visualizing Trends in Multiattribute Transactional Data

### Scope of the project:

We present our temporal clustering-based technique, discuss its algorithmic implementation and performance, demonstrate applications of the technique by analyzing the data in share market.

**Abstract**— Organizations and firms are capturing increasingly more data about their customers, suppliers, competitors, and business environment. Most of this data is multiattribute (multidimensional) and temporal in nature. Data mining and business intelligence techniques are often used to discover patterns in such data; however, mining temporal relationships typically is a complex task. We propose a new data analysis and visualization technique for representing trends in multiattribute temporal data using a clustering-based approach. We introduce Cluster-based Temporal Representation of Event Data (C-TREND), a system that implements the temporal cluster graph construct, which maps multiattribute temporal data to a two-dimensional directed graph that identifies trends in dominant data types over time. In this paper, we present our temporal clustering-based technique, discuss its algorithmic implementation and performance, demonstrate applications of the technique by analyzing data on wireless networking technologies and baseball batting statistics, and introduce a set of metrics for further analysis of discovered trends.

### Modules:

- Transformation of data's from excel sheet
- Creation of dataset
- Partition and clustering
- Dendrogram sorting
- Display the time of sorting.
- Extracting values according to N
- Implementation of JFREE CHART.

## 9. Controlling IP Spoofing through Inter-Domain Packet Filters

### Scope of this project:

IP spoofing is most frequently used in denial-of-service attacks. Packet filtering is one defense against IP spoofing attacks. In this project we are using Border gateway protocol and interdomain packet filter to defense the IP Spoofing.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Introduction:**

Distributed Denial-of-Service (DDoS) attacks pose an increasingly grave threat to the Internet, as evident in recent DDoS attacks mounted on both popular Internet sites and the Internet infrastructure [1]. Alarming, DDoS attacks are observed on a daily basis on most of the large backbone networks [2]. One of the factors that complicate the mechanisms for policing such attacks is IP spoofing, which is the act of forging the source addresses in IP packets. By masquerading as a different host, an attacker can hide its true identity and location, rendering source based packet filtering less effective. It has been shown that a large part of the Internet is vulnerable to IP spoofing

**Modules**

- Constructing Routing Table
- Finding Feasible path
- Constructing Inter-Domain Packet Filters
- Receiving the valid packets

**10. Using the Conceptual Cohesion of Classes for Fault Prediction in Object-Oriented Systems****Scope of the project**

This project will be applicable in well compiled java program and it should have valid comments to measure the cohesion.

**INTRODUCTION**

SOFTWARE modularization, Object-Oriented (OO) decomposition in particular, is an approach for improving the organization and comprehension of source code. In order to understand OO software, software engineers need to create a well-connected representation of the classes that make up the system. Each class must be understood individually and, then, relationships among classes as well. One of the goals of the OO analysis and design is to create a system where classes have high cohesion and there is low coupling among them. These class properties facilitate comprehension, testing, reusability, maintainability, etc.

Software cohesion can be defined as a measure of the degree to which elements of a module belong together. Cohesion is also regarded from a conceptual point of view. In this view, a cohesive module is a crisp abstraction of a concept or feature from the problem domain, usually described in the requirements or specifications. Such definitions, although very intuitive, are quite vague and make cohesion measurement a difficult task, leaving too much room for interpretation. In OO software systems, cohesion is usually measured at the class level and many different OO

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



cohesion metrics have been proposed which try capturing different aspects of cohesion or reflect a particular interpretation of cohesion.

Proposals of measures and metrics for cohesion abound in the literature as software cohesion metrics proved to be useful in different tasks, including the assessment of design quality, productivity, design, and reuse effort, prediction of software quality, fault prediction modularization of software and identification of reusable of components.

Most approaches to cohesion measurement have automation as one of their goals as it is impractical to manually measure the cohesion of classes in large systems. The tradeoff is that such measures deal with information that can be automatically extracted from software and analyzed by automated tools and ignore less structured but rich information from the software (for example, textual information). Cohesion is usually measured on structural information extracted solely from the source code (for example, attribute references in methods and method calls) that captures the degree to which the elements of a class belong together from a structural point of view. These measures give information about the way a class is built and how its instances work together to address the goals of their design. The principle behind this class of metrics is to measure the coupling between the methods of a class. Thus, they give no clues as to whether the class is cohesive from a conceptual point of view (for example, whether a class implements one or more domain concepts) nor do they give an indication about the readability and comprehensibility of the source code. Although other types of metrics were proposed by researchers to capture different aspects of cohesion, only a few metrics address the conceptual and textual aspects of cohesion.

We propose a new measure for class cohesion, named the Conceptual Cohesion of Classes (C3), which captures the conceptual aspects of class cohesion, as it measures how strongly the methods of a class relate to each other conceptually. The conceptual relation between methods is based on the principle of textual coherence. We interpret the implementation of methods as elements of discourse. There are many aspects of a discourse that contribute to coherence, including co reference, causal relationships, connectives, and signals. The source code is far from a natural language and many aspects of natural language discourse do not exist in the source code or need to be redefined. The rules of discourse are also different from the natural language.

C3 is based on the analysis of textual information in the source code, expressed in comments and identifiers. Once again, this part of the source code, although closer to natural language, is still different from it. Thus, using classic natural language processing methods, such as propositional analysis, is impractical or unfeasible. Hence, we use an Information Retrieval (IR) technique, namely, Latent Semantic Indexing (LSI), to extract, represent, and analyze the textual information from the source code. Our

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



measure of cohesion can be interpreted as a measure of the textual coherence of a class within the context of the entire system.

Cohesion ultimately affects the comprehensibility of source code. For the source code to be easy to understand, it has to have a clear implementation logic (that is, design) and it has to be easy to read (that is, good language use). These two properties are captured by the structural and conceptual cohesion metrics, respectively.

#### Modules

- Retrieving the structured information.
- Check the availability of structured information for your source code.
- Apply the LCOM5 formula for structured information.
- Analyze about the comments i.e. unstructured information.
- Index Searching
- Apply the Conceptual similarity formula.
- Comparison

## 11. Mitigating Performance Degradation in Congested Sensor Networks

#### Scope of the project:

Project objective is to lessen the progressive performance failure in an over crowded sensor networks using CAR and MCAR and increase the Delivery Ratio of High-Priority Data

#### Introduction:

SENSOR network deployments may include hundreds or thousands of nodes. Since deploying such large-scale networks has a high cost, it is increasingly likely that sensors will be shared by multiple applications and gather various types of data: temperature, the presence of lethal chemical gases, audio and/or video feeds, etc. Therefore, data generated in a sensor network may not all be equally important. With large deployment sizes, congestion becomes an important problem. Congestion may lead to indiscriminate dropping of data (i.e., high-priority (HP) packets may be dropped while low-priority (LP) packets are delivered). It also results in an increase in energy consumption to route packets that will be dropped downstream as links become saturated. As nodes along optimal routes are depleted of energy, only nonoptimal routes remain, further compounding the problem. To ensure that data with higher priority is received in the presence of congestion due to LP packets, differentiated service must be provided. In this work, we are interested in congestion that results from excessive competition for the wireless medium.

Existing schemes detect congestion while considering all data to be equally

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



important. We characterize congestion as the degradation of service to HP data due to competing LP traffic. In this case, congestion detection is reduced to identifying competition for medium access between HP and LP traffic. Congestion becomes worse when a particular area is generating data at a high rate. This may occur in deployments in which sensors in one area of interest are requested to gather and transmit data at a higher rate than others (similar to bursty converge cast [25]). In this case, routing dynamics can lead to congestion on specific paths. These paths are usually close to each other, which lead to an entire zone in the network facing congestion. We refer to this zone, essentially an extended hotspot, as the congestion zone (Conzone). In this paper, we examine data delivery issues in the presence of congestion. We propose the use of data prioritization and a differentiated routing protocol and/or a prioritized medium access scheme to mitigate its effects on HP traffic. We strive for a solution that accommodates both LP and HP traffic when the network is static or near static and enables fast recovery of LP traffic in networks with mobile HP data sources. Our solution uses a differentiated routing approach to effectively separate HP traffic from LP traffic in the sensor network. HP traffic has exclusive use of nodes along its shortest path to the sink, whereas LP traffic is routed over un-congested nodes in the network but may traverse longer paths. Our contributions in this work are listed as follows:

**Design of Congestion-Aware Routing (CAR):**

CAR is a network-layer solution to provide differentiated service in congested sensor networks. CAR also prevents severe degradation of service to LP data by utilizing un congested parts of the network.

**Design of MAC-Enhanced CAR (MCAR):**

MCAR is primarily a MAC-layer mechanism used in conjunction with routing to provide mobile and lightweight canzone to address sensor networks with mobile HP data sources and/or bursty HP traffic. Compared to CAR, MCAR has a smaller overhead but degrades the performance of LP data more aggressively.

We compare CAR and MCAR to an AODV scheme enhanced with priority queues (AODVpPQ). Both CAR and MCAR lead to a significant increase in the successful packet delivery ratio of HP data and a clear decrease in the average delivery delay compared to AODVpPQ. CAR and MCAR also provide low jitter. Moreover, they use energy more uniformly in the deployment and reduce the energy consumed in the nodes that lie on the Conzone, which leads to an increase in connectivity lifetime. In the presence of sufficient congestion, CAR also allows an appreciable amount of LP data to be delivered. We further show

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



that, in the presence of mobile HP data sources, MCAR provides mobile Conzone, which follow the HP traffic.

**Modules:****1. CAR**

- 1.1 Network Formation
- 1.2 Conzone Discovery
- 1.3 Routing Data via Differentiated paths

**2. MCAR**

- 2.1 Network Formation
- 2.2 Setting Modes
- 2.3 Routing Data

## 12. Location-Based Spatial Query Processing in Wireless Broadcast Environments

**Abstract:**

Location-based spatial queries (LBSQs) refer to spatial queries whose answers rely on the location of the inquirer. Efficient processing of LBSQs is of critical importance with the ever-increasing deployment and use of mobile technologies. We show that LBSQs have certain unique characteristics that the traditional spatial query processing in centralized databases does not address. For example, a significant challenge is presented by wireless broadcasting environments, which have excellent scalability but often exhibit high-latency database access. In this paper, we present a novel query processing technique that, though maintaining high scalability and accuracy, manages to reduce the latency considerably in answering LBSQs. Our approach is based on peer-to-peer sharing, which enables us to process queries without delay at a mobile host by using query results cached in its neighboring mobile peers. We demonstrate the feasibility of our approach through a probabilistic analysis, and we illustrate the appeal of our technique through extensive simulation results.

**Existing System**

- when a mobile user launches a nearest neighbor (NN) query, in many situations, she would prefer an approximate result that arrives with a short response time rather than an accurate result with a long latency.
- The results of spatial queries often exhibit spatial locality. For example, if two MHs are close to each other, the result sets of their spatial queries may overlap significantly. Query results of a mobile peer are valuable for two reasons: 1) they can be used to

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



answer queries of the current MH directly and 2) they can be used to dramatically reduce the latency for the current MH relative to on-air information.

- P2P approaches can be valuable for applications where the response time is an important concern. Through mobile cooperative caching of the result sets, query results can be efficiently shared among mobile clients.

#### **Proposed System:**

- Caching is a key technique to improve data retrieval performance in widely distributed environments. We use a technique called co-operative catching to store the information in requesting MH.
- The next MH which makes a request for same information need not wait for centralized server; it can get reply back from next MH.
- This technique reduces the delay for getting reply for request.
- If even the centralized server is failed, we can get the results from MH.

### **13. intrusion detection in homogeneous and heterogeneous wireless sensor networks**

>>>> analysis phase >>>>

### **14. A Priority-Based MAC Scheduling Algorithm for Enhancing QoS Support in Bluetooth Piconet**

#### **Abstract**

Bluetooth is a personal wireless communication technology and is being applied in many scenarios. Current existing MAC (Medium AccessControl) scheduling scheme only provides best-effort service for all master-slave connections. It is very challenging to provide QoS (Quality of Service) support for different connections due to the feature of Master Driven TDD (Time Division Duplex). This paper addresses the issue of how to enhance QoS support in a Bluetooth piconet. We propose an MAC scheduling algorithm which can provide different QoS for different connections based on priorities. Considering the feature of Master Driven TDD, we define token counters to estimate traffic of real-time slaves. To increase bandwidth utilization, a backoff mechanism is then presented for best-effort slaves to decrease the frequency of polling idle slaves. Simulation results demonstrate that our scheme achieves better performance over the existing schemes.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



## Existing System

In the existing system we consider the Best Effort Connection service in which each client will be scheduled in round robin fashion irrespective of knowing the QOS requirements. The connections which have no data to transmit in both directions belong to this class. This leads to waste of CPU cycles and the bandwidth which leads for unnecessary traffic .

### Limitation of Existing System

- CPU cycles are wasted when the client has no packets to be sent and eventhough it is continuously polled for the packets.
- Bandwidth is utilized improperly which leads for congestion.
- Consumes more time to serve the slaves due to sending of null packets to slaves which do not have polling packets.

### Proposed System

The proposed system consists of both real time connection and the best effort connection. In real time connection, the slaves will be given a unique priority based on its delay requirement. If two connections have same delay requirements, the earlier one will get a priority.

### Advantages of Proposed System

- better QOS performance can be achieved by use of token counters.
- decrease the channel bandwidth wastage caused by polling idle slaves with applying a binary exponential backoff mechanism for polling intervals of best-effort slaves.

## 15. TCP-LP: Low-Priority Service via End-Point Congestion Control

### Abstract

Service prioritization among different traffic classes is an important goal for the Internet. Conventional approaches to solving this problem consider the existing best-effort class as the low-priority class, and attempt to develop mechanisms that provide "better-than-best-effort" service.

We explore the opposite approach, and devise a new distributed algorithm to realize a low-priority service (as compared to the existing best effort)from the network endpoints. To this end, we develop TCP Low Priority (TCP-LP), a distributed algorithm whose goal is to utilize only the excess network bandwidth as compared to the "fair share" of

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



bandwidth as targeted by TCP.

The key mechanisms unique to TCP-LP congestion control are the use of one-way packet delays for early congestion indications and a TCP-transparent congestion avoidance policy. The results of our simulation and Internet experiments show that:

- 1) TCP-LP is largely non-intrusive to TCP traffic.
- 2) Both single and aggregate TCP-LP flows are able to successfully utilize excess network bandwidth; moreover, multiple TCP-LP flows share excess bandwidth fairly
- 3) Substantial amounts of excess bandwidth are available to the low-priority class, even in the presence of "greedy" TCP flows
- 4) Despite their low-priority nature, TCP-LP flows are able to utilize significant amounts of available bandwidth in a wide-area network environment

### Modules

1. Early congestion indication.  
(One-way delay thresholds)
2. Congestion avoidance policy.  
(Additive increase and Multiplicative Decrease)
3. TCP-LP Data transfer
4. TCP-LP Performance Evaluation against TCP

## 16. Distributed & collaborative key agreement Protocols with authentication for dynamic peer groups

### System Analysis:

KEY distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks. In quantum cryptography, quantum key distribution protocols employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. A classical cryptography provides convenient techniques that enable efficient key verification and user authentication. Compared with classical Three-party key distribution protocols, the proposed quantum key distribution protocols easily resist replay and passive attacks. Compared with other quantum key distribution protocols, the proposed schemes efficiently achieve key verification and user authentication and preserve a long term secret key between the TC and each user.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Existing system**

In classical cryptography, three-party key distribution protocols utilize challenge-response mechanisms or timestamps to prevent replay attacks. However, challenge-response mechanisms require at least two communication rounds between the TC and participants, and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to the unpredictable nature of network delays and potential hostile attacks). Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping.

**Proposed system**

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication.

## 17. Provably Secure Three-Party Authenticated Quantum Key Distribution Protocols

**System Analysis:**

KEY distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks. In quantum cryptography, quantum key distribution protocols employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. A classical cryptography provides convenient techniques that enable efficient key verification and user authentication. Compared with classical Three-party key distribution protocols, the proposed quantum key distribution protocols easily resist replay and passive attacks. Compared with other quantum key distribution protocols, the proposed schemes efficiently achieve key verification and user authentication and preserve a long term secret key between the TC and each user.

**Existing system**

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



In classical cryptography, three-party key distribution protocols utilize challenge-response mechanisms or timestamps to prevent replay attacks. However, challenge-response mechanisms require at least two communication rounds between the TC and participants, and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to the unpredictable nature of network delays and potential hostile attacks). Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping.

### **Proposed system**

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication.

## **18. A Distributed Database Architecture for Global Roaming in Next-Generation Mobile Networks**

Global roaming is a basic service of the future mobile networks where terminal mobility, personal mobility and service provider portability must be supported. A non-geographic personal telecommunication number (PTN) for each mobile user is desirable to implement these types of mobile freedom.

### **ABSTRACT**

With location-independent personal telecommunication number PTNs, users can access their personalized services regardless of terminal or attachment point to the network; they can move into different service provider's network and continue to receive subscribed services without changing their PTNs. Another advantage of the flat PTN scheme is that it is much more efficient in terms of capacity than the location-dependent numbering scheme where the capacity of the SN may be exhausted in a highly populated area, whereas the Subscriber Number's (SN) capacity is wasted in a sparsely populated area. However, using the location-independent numbering plan may introduce large centralized databases into a mobile system. To make things worse, each call may require an interrogation to the centralized databases, thus signaling traffic will grow considerably and call setup time may increase dramatically. The large centralized databases may become the bottleneck of the global mobile system, thus

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



necessitating research into the design and performance of high-throughput database technologies as used in mobile networks to meet future demands.

### EXISTING SYSTEM

The database system is a multitree structure, consisting of a number of distributed DSs, each of which is a three-level tree structure. More than three levels may be adopted in a DS. However, adding more levels will introduce longer delays in location registration and call delivery. These DSs communicate with each other only through their root databases, DBOs, which are connected to the PSTN, ATM networks, or other networks.

### PROPOSED SYSTEM

This project proposes a scalable, robust, efficient location database architecture based on the location-independent PTNs. The proposed multitree database architecture consists of a number of database subsystems, each of which is a three-level tree structure and is connected to the others only through its root. By exploiting the localized nature of calling and mobility patterns, the proposed architecture effectively reduces the database loads as well as the signaling traffic incurred by the location registration and call delivery procedures.

## 19. MINIMISING FILE DOWNLOAD TIME IN STOCHASTIC PEER TO PEER NETWORKS

### Abstract

In this paper, we study both positive and negative scale effects on the operations of peer-to-peer (P2P) file sharing networks and propose the optimal sizing (number of peers) and grouping (number of directory intermediary) decisions. Using analytical models and simulation, we evaluate various performance metrics to investigate the characteristics of a P2P network. Our results show that increasing network scale has a positive effect on the expected content availability and transmission cost, but a negative effect on the expected provision and search costs. We propose an explicit expression for the overall utility of a content sharing P2P community that incorporates tradeoffs among all of the performance measures. This utility function is maximized numerically to obtain the optimal network size (or scale). We also investigate the impact of various P2P network parameters on the performance measures as well as optimal scaling decisions. Furthermore, we extend the model to examine the grouping

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



decision in networks with symmetric interconnection structures and compare the performance between random- and location-based grouping policies.

In many ways, the size of a P2P network can impact many of these factors. A large network could alleviate the content reliability problem because the probability of satisfying requested content becomes higher if more peer nodes participate in file sharing activities. It could also reduce transmission delay, on average, as the closest service node will become closer as the network contains more nodes with the same content replica. P2P technologies utilize aggregate bandwidth from edge nodes for content transmission to avoid congestion at dedicated servers. Therefore, the effective bandwidth is scalable with respect to the number of active users. On the other hand, on a large-scale P2P network, the number of queries may cause congestion at directory server (if any) as well as network traffic congestion (one query may be forwarded multiple times before a suitable service node is found), due to limited capacity and network bandwidth. Therefore, determining the "right" network scale is very important for P2P operations.

## 20. Face recognition by eigen values

### Introduction

Face recognition can be applied for a wide variety of problems like image and film processing, human-computer interaction, criminal identification etc. This has motivated researchers to develop computational models to identify the faces, which are relatively simple and easy to implement. The model developed in [1] is simple, fast and accurate in constrained environments. Our goal is to implement the model for a particular face and distinguish it from a large number of stored faces with some real-time variations as well.

The scheme is based on an information theory approach that decomposes face images into a small set of characteristic feature images called 'eigenfaces', which are actually the principal components of the initial training set of face images. Recognition is performed by projecting a new image into the subspace spanned by the eigenfaces ('face space') and then classifying the face by comparing its position in the face space with the positions of the known individuals.

Recognition under widely varying conditions like frontal view, a 45° view, scaled frontal view, subjects with spectacles etc. are tried, while the training data set covers a limited views. Further this algorithm can be extended to recognize the gender of a person or to interpret the facial expression of a person. The algorithm models the real-

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



time varying lighting conditions as well. But this is out of scope of the current implementation.

### **Aim of the project:**

This project is a step towards developing a face recognition system which can recognize static images. It can be modified to work with dynamic images. In that case the dynamic images received from the camera can first be converted in to the static one's and then the same procedure can be applied on them.

### **Scope:**

- 1) To recognize a sample face from a set of given faces .
- 2) Use of Principal Component Analysis [Using Eigenface approach].
- 3) Use a simple approach for recognition and compare it with Eigenface approach .
- 4) Suggest which one is better and why. It may happen that in some cases latter may work better than former approach and vice versa .

## **21. A Distributed Cache Architecture with Snooping for QoS Routing in Large Networks**

### **Abstract**

To meet the diverse quality-of-service (QoS) requirements of emerging multimedia applications, communication networks should provide end-to-end QoS guarantees. QoS routing is the first step towards this goal. The route computing overhead caused by on-demand calculation of QoS routes, especially in large networks with heavy traffic, is a concern and can cause scalability problems. This paper addresses this problem by introducing novel distributed cache architecture. The distributed nature of the proposed cache architecture facilitates its deployment in large networks. To maximize the performance of the distributed cache architecture, cache snooping has been proposed to alleviate the side effects of network states fluctuations on the cached route so that the overall routing performance is significantly improved. Assuming a bandwidth-based QoS model, in performance evaluation of the 4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalsolutions.com](mailto:raghav@goalsolutions.com)



proposed distributed cache architecture, we use a broad range of realistic network topologies, network traffic conditions, routing protocols, and aggregation techniques to evaluate different aspects of the proposed cache architecture under different conditions. The results confirm that the route caching is quite effective in reduction of route computing overhead. In addition, our results suggest that the cache snooping can significantly increase the overall routing performance, especially in the presence of highly inaccurate network state information.

On-demand routing protocols use route caches to make routing decisions. Due to mobility, cached routes easily become stale. To address the cache staleness issue, prior work in DSR used heuristics with ad hoc parameters to predict the lifetime of a link or a route.

The goal of our project is to proactively disseminating the broken link information to the nodes that have that link in their caches. We define a new cache structure called a cache table and present a distributed cache update algorithm. Each node maintains in its cache table the information necessary for cache updates. When a link failure is detected, the algorithm notifies all reachable nodes that have cached the link in a distributed manner. We show that the algorithm outperforms DSR with path caches and with Link-MaxLife, an adaptive timeout mechanism for link caches. We conclude that proactive cache updating is key to the adaptation of on-demand routing protocols to mobility.

#### **Existing network:**

1. TCP performance degrades significantly in Mobile Ad hoc Networks due to the packet losses.
2. Most of these packet losses result from the Route failures due to network mobility.
3. TCP assumes such losses occur because of congestion, thus invokes congestion control mechanisms such as decreasing congestion windows, raising timeout, etc, thus greatly reduce TCP throughput.

#### **Proposed System:**

we propose proactively disseminating the broken link information to the nodes that have that link in their caches. We define a new cache structure called a cache table and present a distributed cache update algorithm. Each node maintains in its cache table the information necessary for cache updates. When a link failure is detected, the algorithm notifies all reachable nodes that have cached the link in a distributed manner. The above problem can be solved through quality-of-service (QoS)

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



## 22. Online handwritten script recognition

### Abstract

Automatic identification of handwritten script facilitates many important applications such as automatic transcription of multilingual documents and search for documents on the Web containing a particular script. The increase in usage of handheld devices which accept handwritten input has created a growing demand for algorithms that can efficiently analyze and retrieve handwritten data. This project proposes a method to classify words and lines in an online handwritten document into one of the six major scripts: Arabic, Cyrillic, Devnagari, Han, Hebrew, or Roman. The classification is based on 11 different spatial and temporal features extracted from the strokes of the words. The proposed system attains an overall classification accuracy of 87.1 percent at the word level with 5-fold cross validation on a data set containing 13,379 words. The classification accuracy improves to 95 percent as the number of words in the test sample is increased to five, and to 95.5 percent for complete text lines consisting of an average of seven words.

### Existing Method

The existing method deals with languages are identified

- Using projection profiles of words and character shapes.
- Using horizontal projection profiles and looking for the presence or absence of specific shapes in different scripts.
- Existing method deals with only few characteristics
- Most of the method does this in off-line

### Proposed System

The proposed method uses the features of connected components to classify six different scripts (Arabic, Chinese, Cyrillic, Devnagari, Japanese, and Roman) and reported a classification accuracy of 88 percent on document pages. There are a few important aspects of online documents that enable us to process them in a fundamentally different way than offline documents. The most important characteristic of online documents is that they capture the temporal sequence of strokes while writing the document. This allows us to analyze the individual strokes and use the additional temporal information for both script identification as well as text recognition. In the case of online documents, segmentation of foreground from the background is a relatively simple task as the captured data, i.e., the (x; y) coordinates of the locus of the stylus, defines the characters and any other point on the page belongs to the background. We use stroke properties as well as the spatial and temporal information of a collection of strokes to identify the script used in the document. Unfortunately, the temporal information also introduces additional variability to the handwritten

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



characters, which creates large intraclass variations of strokes in each of the script classes.

### **23. Image downloading range performance evaluation of java remote method invocation**

#### **ABSTRACT**

With the explosive growth of internet and network services, there is always a proliferation for distributed application that seek to leverage the power of the internet. Remote method invocation is now increasingly being used in Internet based applications and hence it is important to study the performance parameters of RMI. RMI is the action of invoking a method of a remote interface on a remote object. The three methods of RMI namely General , Activation and Custom Socket Factory are to be evaluated empirically using parameters like Round trip time , Latency and Packets per Unit time. The graph plotted allows us to gain an insight into the performance aspects and other tradeoffs of RMI. The General method deals with invoking any method directly from memory of the remote machine. RMI Activation allows passive objects to be brought into the active state by instantiating it on an as needed basis. Custom socket factory method allows customization of socket depending on the type and amount of data to be transferred over the channel. It is proposed to implement security for the data being transferred using Rijndael Algorithm that imparts security due to its high resistance to attacks, code compactness and design simplicity.

### **24. Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes**

#### **Abstract**

This paper reports the design principles and evaluation results of a new experimental hybrid intrusion detection system (HIDS). This hybrid system combines the advantages of low false-positive rate of signature-based intrusion detection system (IDS) and the ability of anomaly detection system (ADS) to detect novel unknown attacks. By mining anomalous traffic episodes from Internet connections, we build an ADS that detects anomalies beyond the capabilities of signature-based SNORT or Bro systems. A weighted signature generation scheme is developed to integrate ADS with SNORT by extracting signatures from anomalies detected. HIDS extracts signatures from the output of ADS and adds them into the SNORT signature database for fast and accurate intrusion detection. By testing our HIDS scheme over real-life Internet trace data mixed with 10 days of Massachusetts Institute of Technology/ Lincoln Laboratory (MIT/LL) attack data set, our experimental results show a 60 percent detection rate of 4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



the HIDS, compared with 30 percent and 22 percent in using the SNORT and Bro systems, respectively. This sharp increase in detection rate is obtained with less than 3 percent false alarms. The signatures generated by ADS upgrade the SNORT performance by 33 percent.

## 25. A Hierarchical Modeling And Analysis For Grid Service Reliability

### ABSTRACT

Grid computing is a recently developed technology. Although the developmental tools and techniques for the grid have been extensively studied.. This paper is the first one that presents a hierarchical model for the grid service reliability analysis and evaluation. The hierarchical modeling is mapped to the physical and logical architecture of the grid service system and makes the evaluation and calculation tractable by identifying the independence among layers. Various types of failures are interleaved in the grid computing environment, such as blocking failures, time-out failures, matchmaking failures, network failures, program failures, and resource failures. This paper investigates all of them to achieve a complete picture about grid service reliability. Markov models, Queuing theory, and Graph theory are mainly used here to model, evaluate, and analyze the grid service reliability. Numerical examples are illustrated.

### EXISTING SYSTEM:

The grid service reliability for a wide-area distributed system that is one of the ancestors of the grid system. The function of the control center in that model is similar to that of RMS for the grid computing. However, the reliability analysis Of the control center is not exactly suitable for the RMS. Moreover, the reliability model of the sub distributed systems inherits the traditional models' characters and has certain limitations. Those traditional models have a common assumption that the operational probabilities of the nodes and links are constant. However, this assumption is unrealistic for the grid, so this assumption was relaxed in by assuming that the failures of nodes and links followed their respective Poisson processes so that their operational probabilities decrease with their working time instead of the constant values. This new model is more reasonable and practical for the grid, but it only studied the network hardware failures for the grid reliability without considering other failures such as blocking failures, timeout failures, matchmaking failures, program failures, and resource failures. There are also many other reliability models for software, hardware, or small-scale distributed systems, which cannot be directly implemented for studying grid service reliability.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



## PROPOSED SYSTEM

The services in proposed grid systems are often organized in a hierarchical fashion: They contain different program/ resource/request/network/management layers that are interconnected through a set of interfaces. The reliability characteristics of some lower layers are largely independent of the layers above. From the system's perspective, the whole grid is also built from smaller, more manageable subsystems (such as the component-based approach). This characteristic of large scale systems fits naturally in the hierarchical modeling approach that is adopted by this paper.

The proposed system focuses on making better and cost effective use of existing computing power and resources with the view to share applications and collaborate on projects through distributed computing.

A grid computing system is a distributed parallel collection of computers that enables the sharing, selection and aggregation of resources. This sharing is based on the resources' availability, capability, performance, cost and ability to meet quality-of-service requirements. The Grid merges people, computers, databases, instruments, and other resources in ways that were simply never possible before.

By using an agent enhanced Search Engine with grid technology, the customer requirements can be satisfied by searching for the required data and retrieving the results in real time. At the same time, it improves the resource usage and provides efficient workload optimization

## 26.SLA-Driven Clustering of QoS-Aware Application Servers

### Objective:

To developed a middleware architecture that can be integrated in an application server to allow it to honor the SLAs of the applications it hosts—in other words, to make it QoS-aware. The architecture guaranteeing that the QoS requirements specified in SLAs are met, Optimizing the resource utilization in addressing item and Maximizing the portability of the software architecture across a variety of specific J2EE implementations

### Abstract:

In this paper, we discuss the design, implementation, and experimental evaluation of a middleware architecture for enabling Service Level Agreement (SLA)-driven clustering of QoS-aware application servers. Our middleware architecture supports application server technologies with dynamic resource management: Application servers can dynamically change the amount of clustered resources assigned to hosted applications on-demand so as to meet application-level Quality of Service (QoS) requirements. These requirements can include timeliness, availability, and high

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



throughput and are specified in SLAs. A prototype of our architecture has been implemented using the open-source J2EE application server JBoss. The evaluation of this prototype shows that our approach makes possible JBoss' resource usage optimization and allows JBoss to effectively meet the QoS requirements of the applications it hosts, i.e., to honor the SLAs of those applications.

### **System Analysis:**

Distributed enterprise applications (e.g., stock trading, business-to-business applications) can be developed to be run with application server technologies such as Java 2 Enterprise Edition (J2EE) servers, CORBA Component Model (CCM) servers, or .NET . These technologies can provide the applications they host with an execution environment that shields those applications from the possible heterogeneity of the supporting computing and communication infrastructure; in addition, this environment allows hosted applications to openly access enterprise information systems, such as legacy databases.

These applications may exhibit strict Quality of Service (QoS) requirements, such as timeliness, scalability, and high availability, that can be specified in so-called Service Level Agreements (SLAs). SLAs are legally binding contracts that state the QoS guarantees an execution environment has to supply its hosted applications.

### **Existing System:**

Current application server technology offers clustering and load balancing support that allows the application designer to handle scalability and high availability application requirements at the application level; however, this technology is not fully tailored to honor possible SLAs.

In order to overcome this limitation, we have developed a middleware architecture that can be integrated in an application server to allow it to honor the SLAs of the applications it hosts—in other words, to make it QoS-aware. The designed architecture supports dynamic clustering of QoS-aware Application Servers (QaAs) and load balancing.

In current J2EE servers, the clustering support is provided in the form of a service. In general, that service requires the initial cluster configuration to consist of a fixed set of application server instances. In the case of peak load conditions or failures, this set of instances can be changed at runtime by a human operator reconfiguring the cluster as necessary (e.g., by introducing new server instances or by replacing failed instances). In addition, current clustering support does not include mechanisms to guarantee that application-level QoS requirements are met. These limitations can impede the efficient use of application server technologies in a utility computing context. In fact, current clustering design requires overprovision policies to be used

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



in order to cope with variable and unpredictable load and prevent QoS requirements violations.

### Proposed System:

Our middleware architecture is principally responsible for the dynamic configuration, runtime monitoring, and load balancing of a QoS-aware cluster. It operates transparently to the hosted applications (hence, no modifications to these applications are required) and consists of the following three main services: Configuration Service, Monitoring Service, and Load Balancing Service.

In our proposed system we implement the Service Level Agreement (SLA) Concept using WegLogic Application server, which is highly reliable than JBoss Server and then we implement the concept of Load Balancing logically and not the implement the existing load balancing resources that already available in JBoss server.

We have developed a software architecture that allows dynamic J2EE application server clustering and automatic cluster reconfiguration at runtime. Our architecture allows a J2EE cluster to react to possible changes of its own operational conditions that could result in violations of application QoS requirements.

## 27. HIDING SENSITIVE ASSOCIATION RULES WITH MINIMUM SIDE EFFECTS

### Abstract

Data mining techniques have been widely used in various applications. However, the misuse of these techniques may lead to the disclosure of sensitive information. Researchers have recently made efforts at hiding sensitive association rules. Nevertheless, undesired side effects, e.g., no sensitive rules falsely hidden and spurious rules falsely generated, may be produced in the rule hiding process. In this paper, we present a novel approach that strategically modifies a few transactions in the transaction database to decrease the supports or confidences of sensitive rules without producing the side effects. Since the correlation among rules can make it impossible to achieve this goal, in this paper, we propose heuristic methods for increasing the number of hidden sensitive rules and reducing the number of modified entries. The experimental results show the effectiveness of our approach, i.e., undesired side effects are avoided in the rule hiding process. The results also report that in most cases, all the sensitive rules are hidden without spurious rules falsely generated. Moreover, the good scalability of our approach in terms of

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



database size and the influence of the correlation among rules on rule hiding are observed.

## 28. Cryptographic Versus Trust-based Methods for MANET Routing Security

### ABSTRACT

Mobile Ad-hoc Networks (MANETs) allow wireless nodes to form a network without requiring a fixed infrastructure. Early routing protocols for MANETs failed to take security issues into account. Subsequent proposals used strong cryptographic methods to secure the routing information. In the process, however, these protocols created new avenues for denial of service (DoS). Consequently, the trade-off between security strength and DoS vulnerability has emerged as an area requiring further investigation. It is believed that different trust methods can be used to develop protocols at various levels in this trade-off. To gain a handle on this exchange, real world testing that evaluates the cost of existing proposals is necessary. Without this, future protocol design is mere speculation. In this paper, we give the first comparison of SAODV and TAODV, two MANET routing protocols, which address routing security through cryptographic and trust-based means respectively. We provide performance comparisons on actual resource-limited hardware. Finally, we discuss design decisions for future routing protocols.

Key words: mobile, ad-hoc, security, routing, cryptography, trust-based, performance

## 29. An Efficient and Secure Content Processing and Distribution by Cooperative Intermediaries

### Scope of the project:

In this project we are going to permit multiple intermediaries to simultaneously perform content service on different portion data. Our protocol supports decentralized proxy and key management and flexible delegation of services. Our experimental results show that our approach is efficient and minimizes the amount of data transmitted across the network.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Introduction:**

In order to enhance the performance of content distribution networks (CDNs), several approaches have been developed based on the use of content management services provided by intermediary proxies. In most of these approaches, content caching is the main service provided by proxies. That is, instead of asking a content server for contents upon each client request, a proxy first checks if these contents are locally cached. Only when the requested contents are not cached or out of date are the contents transferred from the content server to the clients. If there is a cache hit, the network bandwidth consumption can be reduced. A cache hit also reduces access latency for the clients. System performance thus improves, especially when a large amount of data is involved. Besides these improvements, caching makes the system robust by letting caching proxies provide content distribution services when the server is not available.

**Modules:**

**Client Module** This is any entity that requests data from a data server. When a client submits a request, besides the data it requests, it may also include some content service requirements, arising from device limitations and data format limitations

**Intermediate Server Module**

This is any entity that is allowed by a data server to provide content services in response to requests by clients. Intermediaries include caching proxies and transforming proxies.

**Data Server Module** This is an entity that originally stores the data requested by a client.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



### 30. Problem Oriented Software Engineering: Solving the Package Router Control Problem

Abstract—Problem orientation is gaining interest as a way of approaching the development of software intensive systems, and yet, a significant example that explores its use is missing from the literature. In this paper, we present the basic elements of Problem Oriented Software Engineering (POSE), which aims at bringing both nonformal and formal aspects of software development together in a single framework. We provide an example of a detailed and systematic POSE development of a software problem: that of designing the controller for a package router. The problem is drawn from the literature, but the analysis presented here is new. The aim of the example is twofold: to illustrate the main aspects of POSE and how it supports software engineering design and to demonstrate how a nontrivial problem can be dealt with by the approach.

SOFTWARE engineering includes the identification and clarification of system requirements, the understanding and structuring of the problem world, the structuring and specification of a hardware/software machine that can ensure the satisfaction of the requirements in the problem world, and the construction of adequacy arguments, convincing both to developers and to customers, users, and other interested parties, that the system will provide what is needed. These activities are much concerned with nonformal domains of reasoning: the physical and human world, requirements expressed in a natural language, the capabilities of human users and operators, and the identification and resolution of apparent and real conflicts between different needs. In a software-intensive system, these informal domains interact with the essentially formal hardware/software machine: An effective approach to system development must therefore deal adequately with the nonformal, the formal, and the relationships between them. As Turski has pointed out [1]: "There are two fundamental difficulties involved in dealing with nonformal domains

### 31. A secure manet routing protocol for detecting faulty links

#### Abstract

We study routing misbehavior in MANETs (Mobile Ad Hoc Networks) in this paper. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.

### 32. PC remote

This is a project to control the PC using Bluetooth enabled mobile phone through Bluetooth connectivity. Once the PC and the mobile phone are synchronized, the mobile provides many options to control and access the PC. The PC can be turned off, restarted, logged off and successfully browsed through the connected mobile phone. While browsing the PC, any files and folders can be opened, renamed and deleted. The File/folder can also be copied and moved from one directory to another.

When a file is opened through mobile phone, it is opened with its default application in PC. In case of folder, it is explored in desktop and the contents will be listed in the mobile phone.

Mobile phone can be used as Bluetooth mouse. Mouse arrow is controlled through mobile phone keys.

### 33. Load Balancing in Distributed VoD using Local Proxy Server Group [LPSG]

**Introduction:** In computer networks, a proxy server is a server (a computer system or an application program) which services the requests of its clients by forwarding requests to other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server provides the resource by connecting to the specified server and requesting the service on behalf of the client. For the first time the proxy server would connect to the main server and serve the client request. Meanwhile it would 'cache' the result of the request in its local buffer. And it uses this information for subsequent requests without connecting to the main server so that it reduces the bandwidth requirement and increases the accessing speed.

This feature of the proxy server can also be used for load balancing in Distributed VoD (Video on Demand) since in recent years, requirement is to reduce the waiting time and bandwidth demand between the Central Multimedia Server (CMS) and client. Proxy servers can be used for multimedia contents to decrease the waiting time and to reduce the load of the CMS.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



In this paper, a new load sharing algorithm and a new VoD architecture is proposed for distributed VoD system. The architecture consists of a CMS which is connected to a group of trackers. Each tracker is in turn connected to a set of proxy servers and these proxy servers are assumed to be interconnected in a ring fashion. The proposed VoD architecture is as shown Fig.1. The proxy server caches the video content currently requested by its users. The tracker is a coordinating proxy server, which maintains a database that contains the information of the videos present in each proxy server in that LPSG [Local Proxy Servers Group].

### 35. PreActive circulated cache updating using dynamic source routing protocol

**Abstract** On-demand routing protocols use route caches to make routing decisions. Due to mobility, cached routes easily become stale. To address the cache staleness issue, prior work in DSR used heuristics with ad hoc parameters to predict the lifetime of a link or a route.

The goal of our project is to proactively disseminating the broken link information to the nodes that have that link in their caches. We define a new cache structure called a cache table and present a distributed cache update algorithm. Each node maintains in its cache table the information necessary for cache updates. When a link failure is detected, the algorithm notifies all reachable nodes that have cached the link in a distributed manner. We show that the algorithm outperforms DSR with path caches and with Link-MaxLife, an adaptive timeout mechanism for link caches. We conclude that proactive cache updating is key to the adaptation of on-demand routing protocols to mobility.

The modules that are included in this project are

- Route Request
- Route Maintenance
- Message Transfer
- Cache Update

### 36. DYNAMIC SOURCE ROUTING USING LAR PROTOCOL

#### abstract

An ad-hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



between nodes are capable of changing on a continual basis. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. LAR is an on-demand protocol who is based on the DSR(Dynamic Source Routing). The Location Aided Routing protocol uses location information to reduce routing overhead of the ad-hoc network! Normally the LAR protocol uses the GPS(Gloal Positioning System) to get these location informations. With the availability of GPS, the mobile hosts knows there physical location.

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of the network topology. Figure 1 shows such an example: initially, nodes A and D have a direct link between them. When D moves out of A's radio range, the link is broken. However, the network is still connected, because A can reach D through C, E, and F. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad hoc network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

### 37. Effective packet analyzing & filtering system for ATM Networks

**ABSTRACT** The objective of this project is to simulate an overflowing ATM network and establish a router with congestion control based on the GCRA algorithm.

The TCP/IP protocol suite is the standard requirement for all applications that need to communicate over the Internet. As TCP/IP applications are unable to specify the QoS parameters needed for most Asynchronous Transfer Mode (ATM) services, we tend to use the GCRA Algorithm.

The purpose of Cell-Rate Guarantees for Traffic across ATM Network is to provide QoS. ATM is a connection-oriented switching technology, utilizing statistical multiplexing of fixed-length packets, known as cells.

The purpose of traffic control is to minimize congestion. In an ATM network when the Source Machine continuously sends cells to the Destination Machine through the Router Machine, there will be a possibility of occurring congestion. When congestion occurs the Routing Machine cannot accept more cells and hence these cells will be discarded. This causes regeneration and retransmission of the discarded ATM cells.

#### Existing System

In the existing system when transferring data from sender to receiver there may be chances of data loss. No user can be known whether the router is free after he sends data to the router. Also no intimation when the buffer at the router is full or busy or free. It causes retransmission of data to the router and hence redundant bandwidth usage and consumption of time.

#### Proposed System

In this System, using several algorithms viz. Leaky bucket algorithm and Virtual scheduling algorithm congestion can be avoided. Leaky Bucket Algorithm continuously receives and sends the data at the particular interval of time to avoid congestion or flooding of data. Virtual scheduling algorithm monitors the congestion occurrence, when congestion occurs it intimates or warns user and simultaneously intimates when the router is free and data transferred successfully to destination.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



### 38. dynamic search algorithm in unstructured peer to peer >>> analysis phase>>>

### 39. Efficient and Secure Content Processing and Distribution by Cooperative Intermediaries

#### Scope of the project:

In this project we are going to permit multiple intermediaries to simultaneously perform content service on different portion data. Our protocol supports decentralized proxy and key management and flexible delegation of services. Our experimental results show that our approach is efficient and minimizes the amount of data transmitted across the network.

#### Introduction:

In order to enhance the performance of content distribution networks (CDNs), several approaches have been developed based on the use of content management services provided by intermediary proxies. In most of these approaches, content caching is the main service provided by proxies. That is, instead of asking a content server for contents upon each client request, a proxy first checks if these contents are locally cached. Only when the requested contents are not cached or out of date are the contents transferred from the content server to the clients. If there is a cache hit, the network bandwidth consumption can be reduced. A cache hit also reduces access latency for the clients. System performance thus improves, especially when a large amount of data is involved. Besides these improvements, caching makes the system robust by letting caching proxies provide content distribution services when the server is not available.

#### Modules:

**Client Module** This is any entity that requests data from a data server. When a client submits a request, besides the data it requests, it may also include some content service requirements, arising from device limitations and data format limitations

**Intermediate Server Module** This is any entity that is allowed by a data server to provide content services in response to requests by clients. Intermediaries include caching proxies and transforming proxies.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Data Server Module** This is an entity that originally stores the data requested by a client.

#### 40. Probabilistic Packet Marking For Large Scale IP Trace Back

##### Scope

This project will be applicable in secured data sharing in the structured network.

##### Introduction

THE denial-of-service (DoS) attack has been a pressing problem in recent years. DoS defense research has blossomed into one of the main streams in network security. Various techniques such as the pushback message, ICMP traceback, and the packet filtering techniques are the results from this active field of research. The probabilistic packet marking (PPM) algorithm by Savage et al. has attracted the most attention in contributing the idea of IP traceback. The most interesting point of this IP traceback approach is that it allows routers to encode certain information on the attack packets based on a predetermined probability. Upon receiving a sufficient number of marked packets, the victim (or a data collection node) can construct the set of paths that the attack packets traversed and, hence, the victim can obtain the location(s) of the attacker(s).

The Probabilistic Packet Marking Algorithm The goal of the PPM algorithm is to obtain a constructed graph such that the constructed graph is the same as the attack graph, where an attack graph is the set of paths the attack packets traversed, and a constructed graph is a graph returned by the PPM algorithm. To fulfill this goal, Savage et al. Suggested a method for encoding the information of the edges of the attack graph into the attack packets through the cooperation of the routers in the attack graph and the victim site. Specifically, the PPM algorithm is made up of two separated procedures: the packet marking procedure, which is executed on the router side, and the graph reconstruction procedure, which is executed on the victim side.

The packet marking procedure is designed to randomly encode edges' information on the packets arriving at the routers. Then, by using the information, the victim executes the graph reconstruction procedure to construct the attack graph. We first briefly review the packet marking procedure so that readers can become familiar with how the router marks information on the packets

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Existing System:-**

- In the existing system PPM algorithm is not perfect, as its termination condition is not well defined.
- The algorithm requires prior knowledge about the network topology.
- In packet marking algorithm the Termination Packet Number(TPN) calculation is not well defined in the literature.
- In the existing system it only supports the single attacker environment.

**Dis-Advantages of Existing System**

- Without proper termination condition the attack graph constructed by the PPM algorithm would be wrong.
- The constructed path and the re-construction will be differed.
- It won't support the multiple attacker environments.

**Proposed System:-**

- To propose termination condition of the PPM algorithm, this is missing or is not explicitly defined in the literature.
- Through the new termination condition, the user of the new algorithm is free to determine the correctness of the constructed graph.
- The constructed graph is guaranteed to reach the correctness assigned by the user, independent of the marking probability and the structure of the underlying network graph.
- In this system we proposed a Rectified Probabilistic Packet Marking Algorithm to encode the packet in the routers to detect the attacked packets.
- To reduce the a constructed graph such that the constructed graph is the same as the attack graph, where an attack graph is the set of paths the attack packets traversed,
- To construct a graph, is a graph returned by the PPM algorithm.

#### 41. Evaluation Of Middle Ware Architecture For Enabling Service Level Agreement Application Servers

**Objective:**

To developed a middleware architecture that can be integrated in an application server to allow it to honor the SLAs of the applications it hosts—in other words, to make it QoS-aware. The architecture guaranteeing that the QoS requirements specified in SLAs are met, Optimizing the resource utilization in addressing

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



item and Maximizing the portability of the software architecture across a variety of specific J2EE implementations

**Abstract:**

In this paper, we discuss the design, implementation, and experimental evaluation of a middleware architecture for enabling Service Level Agreement (SLA)-driven clustering of QoS-aware application servers. Our middleware architecture supports application server technologies with dynamic resource management: Application servers can dynamically change the amount of clustered resources assigned to hosted applications on-demand so as to meet application-level Quality of Service (QoS) requirements. These requirements can include timeliness, availability, and high throughput and are specified in SLAs. A prototype of our architecture has been implemented using the open-source J2EE application server JBoss. The evaluation of this prototype shows that our approach makes possible JBoss' resource usage optimization and allows JBoss to effectively meet the QoS requirements of the applications it hosts, i.e., to honor the SLAs of those applications.

**Existing System:**

Current application server technology offers clustering and load balancing support that allows the application designer to handle scalability and high availability application requirements at the application level; however, this technology is not fully tailored to honor possible SLAs.

In order to overcome this limitation, we have developed a middleware architecture that can be integrated in an application server to allow it to honor the SLAs of the applications it hosts—in other words, to make it QoS-aware. The designed architecture supports dynamic clustering of QoS-aware Application Servers (QaASs) and load balancing.

In current J2EE servers, the clustering support is provided in the form of a service. In general, that service requires the initial cluster configuration to consist of a fixed set of application server instances. In the case of peak load conditions or failures, this set of instances can be changed at runtime by a human operator reconfiguring the cluster as necessary (e.g., by introducing new server instances or by replacing failed instances). In addition, current clustering support does not include mechanisms to guarantee that application-level QoS requirements are met. These limitations can impede the efficient use of application server technologies in a utility computing context. In fact, current clustering design requires overprovision policies to be used in order to cope with variable and unpredictable load and prevent QoS requirements violations.

**Proposed System:**

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



Our middleware architecture is principally responsible for the dynamic configuration, runtime monitoring, and load balancing of a QoS-aware cluster. It operates transparently to the hosted applications (hence, no modifications to these applications are required) and consists of the following three main services: Configuration Service, Monitoring Service, and Load Balancing Service.

In our proposed system we implement the Service Level Agreement (SLA) Concept using WegLogic Application server, which is highly reliable than JBoss Server and then we implement the concept of Load Balancing logically and not the implement the existing load balancing resources that already available in JBoss server.

We have developed a software architecture that allows dynamic J2EE application server clustering and automatic cluster reconfiguration at runtime. Our architecture allows a J2EE cluster to react to possible changes of its own operational conditions that could result in violations of application QoS requirements.

#### **42. Efficient key management for threshold multisignature in distributed systems**

**abstract**—Threshold-multisignature schemes combine the properties of threshold group-oriented signature schemes and multisignature schemes to yield a signature scheme that allows a threshold ( $t$ ) or more group members to collaboratively sign an arbitrary message. In contrast to threshold group signatures, the individual signers do not remain anonymous, but are publicly identifiable from the information contained in the valid threshold-multisignature. The main objective of this paper is to propose such a secure and efficient threshold-multisignature scheme. The paper uniquely defines the fundamental properties of threshold-multisignature schemes and shows that the proposed scheme satisfies these properties and eliminates the latest attacks to which other similar schemes are subject. The efficiency of the proposed scheme is analyzed and shown to be superior to its counterparts.

The paper also proposes a discrete logarithm based distributed-key management infrastructure (DKMI), which consists of a round optimal, publicly verifiable, distributed-key generation (DKG) protocol and a one round, publicly verifiable, distributed-key redistribution

updating (DKRU) protocol. The round optimal DKRU protocol solves a major problem with existing secret redistribution/updates schemes by giving group members a mechanism to identify malicious or faulty share holders in the first round, thus avoiding multiple protocol executions.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



### 43. Intruder detection system over abnormal internet sequence

#### Abstract

This paper reports the design principles and evaluation results of a new experimental hybrid intrusion detection system (HIDS). This hybrid system combines the advantages of low false-positive rate of signature-based intrusion detection system (IDS) and the ability of anomaly detection system (ADS) to detect novel unknown attacks. By mining anomalous traffic episodes from Internet connections, we build an ADS that detects anomalies beyond the capabilities of signature-based SNORT or Bro systems. A weighted signature generation scheme is developed to integrate ADS with SNORT by extracting signatures from anomalies detected. HIDS extracts signatures from the output of ADS and adds them into the SNORT signature database for fast and accurate intrusion detection. By testing our HIDS scheme over real-life Internet trace data mixed with 10 days of Massachusetts Institute of Technology/ Lincoln Laboratory (MIT/LL) attack data set, our experimental results show a 60 percent detection rate of the HIDS, compared with 30 percent and 22 percent in using the SNORT and Bro systems, respectively. This sharp increase in detection rate is obtained with less than 3 percent false alarms. The signatures generated by ADS upgrade the SNORT performance by 33 percent.

The HIDS approach proves the vitality of detecting intrusions and anomalies, simultaneously, by automated data mining and signature generation over Internet connection episodes.

### 44. The plagiarism hunter

#### Abstract:

Several tools are marketed to the educational community for plagiarism detection and prevention. The proposed System contrasts the performance of two leading tools, TurnItIn and MyDropBox, in detecting submissions that were obviously plagiarized from articles published in IEEE journals. Both tools performed poorly because they do not compare submitted writings to publications in the IEEE database. Reports from these tools suggesting that a submission has "passed" can encourage false confidence in the integrity of a submitted writing. Additionally, students can submit drafts to determine the extent to which these tools detect plagiarism in their work.. An appearance of

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



successful plagiarism prevention may in fact reflect better training of students to avoid plagiarism detection.

#### EXISTING SYSTEM:

- TurnItIn works by comparing writings to articles in its proprietary database and in some commercial or academic databases.
- If a given article is published in a journal not in the TurnItIn database, has not been posted on the Web, and has not been submitted to TurnItIn for a plagiarism check in a way that allows TurnItIn to archive a copy of it, a plagiarized section of that article will not be detected by TurnItIn.
- The TurnItIn website does not make clear which professional databases are included and which are excluded from their indexing.
- These services might miss most plagiarism from the professional-level publication in software engineering.

#### PROPOSED SYSTEM:

- It checks entire educational database
- It gives clear reports base on the plagiarism deduction service reports.
- It also give comments and feedback about the work
- It is mainly for professional level , and students can improve his experimental work.
- Its result is highly accurate when compared to the existing tool.

#### 45.Truth Discovery with Multiple Conflicting Information Providers on the Web.

##### Abstract

The world-wide web has become the most important information source for most of us. Unfortunately, there is no guarantee for the correctness of information on the web. Moreover, different web sites often provide conflicting information on a subject, such as different specifications for the same product. In this paper we propose a new problem called Veracity that is conformity to truth, which studies how to find true facts from a large amount of conflicting information on many subjects that is provided by various web sites. We design a general framework for the Veracity problem, and invent an algorithm called Truth Finder, which utilizes the relationships between web sites and their information, i.e., a web site is trustworthy if it provides many pieces of true information, and a piece of information is likely to be true if it is provided by many trustworthy web sites. Our experiments show that Truth Finder successfully finds true facts

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



among conflicting information, and identifies trustworthy web sites better than the popular search engines.

### **System Analysis**

#### **Existing System**

- Page Rank and Authority-Hub analysis is to utilize the hyperlinks to find pages with high authorities.
- These two approaches identifying important web pages that users are interested in, Unfortunately, the popularity of web pages does not necessarily lead to accuracy of information.

#### **Disadvantage**

1. The popularity of web pages does not necessarily lead to accuracy of information.
2. Even the most popular website may contain many errors.
3. Where as some comparatively not-so-popular websites may provide more accurate information.

#### **Proposed System**

1. We formulate the Veracity problem about how to discover true facts from conflicting information.
2. Second, we propose a framework to solve this problem, by defining the trustworthiness of websites, confidence of facts, and influences between facts.
3. Finally, we propose an algorithm called TRUTHFINDER for identifying true facts using iterative methods.

#### **Advantage**

1. Our experiments show that TRUTHFINDER achieves very high accuracy in discovering true facts.
2. It can select better trustworthy websites than authority-based search engines such as Google.

## **46.Speeding up Secure Web Transactions Using Identity Based Cryptography**

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**ABSTRACT** Secure communication is an intrinsic requirement of today's world of on-line transactions. Whether exchanging financial, business or personal information, people want to know with whom they are communicating (authentication) and they wish to ensure that the information is neither modified (data integrity) nor disclosed (confidentiality) in transit. The growing popularity of web applications in the last few years has led users to give the management of their data to online application providers, which will endanger the security and privacy of the users. In this project, we present WebIBC, which integrates public key cryptography into web applications without any browser plugins. The implementation and performance evaluation demonstrate that WebIBC is secure and efficient both in theory and practice.

#### **Existing System:**

- In existing system, security is achieved through certificate management and certificate authority by using traditional Public Key Cryptography.
- The public key authentication will increase the communication cost and storage capacity.

#### **PROPOSED SYSTEM:**

- Enhancing web application with web Identity Based Cryptography and Private Key Generator( Trusted Authority)
- Every user needs to authenticate him to authority by providing some credentials he has owned the identity, and the authority will extract the private key from the master secret according to user's identity.
- The public and private key pair is generated using Elliptic Curve Cryptography (ECC)
- It should be noticed that all the cryptography operations are all done within the browser, and the server can only receive the cipher text. The security and privacy of end users can be protected from attacks both on network and server side. From another point of view, server is also free from the burden of cryptography operations which means WebIBC is a good model for distributed computation based on web browsers.

### **47.An Efficient Approach for NAT Traversal Problem on Security of Voice over Internet Protocol**

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



**Abstract** This paper evaluates an efficient approach for Network Address Translation (NAT) problem on Voice over Internet Protocol (VoIP) network system. Based on our experiment, we examined the latency, buffer size and voice packet loss under various network conditions. We found that it is possible to establish a call from outside the NAT to inside maintaining the quality issues of VoIP call. With this approach it is possible to use the current network architecture with having few changes in the registrar server. Based on this result, we propose a model for VoIP system that eliminates NAT traversal problem of VoIP call setup. Hence we evaluate our model showing the QoS conditions that achieves both high efficiency and secure voice transmission.

### Existing System

- In the existing system Network Address Translation (NAT) problem was handled by UPnP, STUN, TURN.
- But in that system, they can't give the complete solution for the NAT. In the Universal Plug and Play (UPnP) is that it will not work in the case of cascading NATs.
- The defect of Simple Traversal of User Datagram Protocol through Network Address Translators (STUN) is that it can't work with symmetric NAT, which is widely used in today's enterprise. Therefore STUN can't provide a complete solution.
- Traversal Using Relay NAT (TURN) It is a feasible way to pass through all kinds of NAT, but it also comes at high cost to the provider of the TURN server.

### Dis-advantages

- TURN does not allow for users to run servers on well known ports if they are behind a NAT.
- It supports the connection of a user behind a NAT to only a single peer.
- UPnP does not support multiple network environment while sharing the data. It also having some problem while network address mapping.

### Proposed System

- We have proposed a solution for establishing sessions using SIP through NAT.
- An efficient approach called Traversal Using Keep Alive Binding is designed for implementing at both the end devices and the modifying the Location server.
- Traversal Using Keep Alive Binding can find the shortest paths for the media sessions with only a trivial overhead.
- We believe, the Traversal Using Keep Alive Binding is committed to providing a next generation network that provides both full multi-vendor interoperability, and support for a full featured, secure PSTN service.

### Advantages

- It is necessary to initiate sessions from public networks into a private network.

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



- It also requires modifying the address information in the SIP messages into a reachable one.
- These problems are resolved in our model and the overall efficiency is improved.

## 50. File-Sharing versus Gift-Giving: a Theoretical Approach

**ABSTRACT** To date, online music file-sharing has been considered as one of the most drastic revolution of consumption in the history of record industries. Due to its rapid expansion as a phenomenon, contradictory opinions were articulated over its character, its identity and its results in the music industry field. The consideration of file-sharing is a substitute for the purchase of original albums or a special category of gift exchange is the basic reason for the failure of record industries to eliminate the downloading procedure from unauthorized peer-to-peer networks and to successfully incorporate this practice within their marketing practices. One of the contrapositions studied in the present paper is the comparison of file sharing with the process of gift-giving, considering this connection as simplistic and metaphorical.

Many investigations have tried to depict the character of music file-sharing, identifying it with gift giving, without explaining the connection but what kind of gift-giving procedure it is. It is believed that this identification is rather simplistic and in order to show the identity of both activities a comparison between them is reported, presenting a threefold categorization of differences in terms of product properties, procedure, and motives. It results that file sharing is not gift-giving and that digital music has mostly the characteristics of a socially redistributed public good.

### EXISTING SYSTEM:

In the existing literature concerning file sharing, the approach is parasitic in nature. In NAPSTER file sharing is done in the parasitic way. When the peers in need of a file will search it and find it from another peer then they grab from the donor peer without any permission. Even while downloading a file, if a peer goes offline the total file seems to be corrupted. In NAPSTER peer – peer architecture is followed, which is unsecured and unstructured, so it allows anonymous users or 'leechers' or freeloader to collapse the whole network, by sending or destroying the resources.

### PROPOSED SYSTEM:

In order to adequately frame the different procedures that are generated during the two activities, a comparison between Sherry's model of gift-giving process and the file-sharing activity will be presented. The intention is to show possible connections and deviations that online file-sharing has from each of the three stages of gift-giving gestation, presentation and reformulation. In our

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)



approach we followed a structured peer – peer architecture to preventing from 'leechers' to collide the whole network. Here the file sharing is done in similar to the gift giving process. We also carefully prepared the process by without having any harming or 0% loss for both recipient and especially to the donor.

### 51.A Signature-Based Indexing Method for Efficient Content-Based Retrieval of Relative Temporal Patterns

**Abstract:** A number of algorithms have been proposed for the discovery of data's from the large database. However, since the number of generated patterns can be large, selecting which patterns to analyze can be nontrivial. There is thus a need for algorithms and tools that can assist in the selection of discovered patterns so that subsequent analysis can be performed in an efficient and, ideally, interactive manner. In this project, we propose a signature-based indexing method to optimize the storage and retrieval of a relative data's from the large database.

#### Existing Systems:

- ❖ Inverted Files indexing method concentrate partial match retrieval, which are basically subset queries.
- ❖ An inverted list that stores a list of references to all occurrences of this value in the database

#### Proposed System:

- Focuses on supporting content-based queries of data's from the database.
- Efficiently can be retrieved by signature file indexing method

4<sup>th</sup> floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

[raghav@goalitsolutions.com](mailto:raghav@goalitsolutions.com)

