

2009 DOT NET LIST & ABSTRACTS

1. Probabilistic Packet Marking for Large-Scale IP Trace back
2. On Guaranteed Smooth Switching for Buffered Crossbar Switches
3. Efficient Broadcasting Using Store mix forward method
4. Incentive-Based Scheduling for Market-Like Computational Grids
5. Rate less Forward Error Correction for Topology-Transparent Scheduling
6. HBA:Distributed Metadata Management for Large Cluster-Based Storage Systems
7. Minimizing File Download Time in Stochastic Peer to-Peer Networks
8. Statistical Techniques for Detecting Traffic Anomalies Through Packet Header Data
9. A Geometric Approach to Improving Active Packet Loss Measurement
10. A Cost-Based Approach to Adaptive Resource Management in Data Stream Systems
11. Watermarking Relational Databases Using Optimization-Based Techniques
12. Rough sets-based Search engine for grid service discovery
13. Analyzing and Managing Role-Based Access Control Policies
14. Hardware-Enhanced Association Rule Mining with Hashing and Pipelining
15. Trustworthy Computing under Resource Constraints with the DOWN Policy
16. Securing User-Controlled Routing Infrastructures
17. Credit Card Fraud Detection Using Hidden Markov Model

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



Excellence and Innovation

ABSTRACTS

1. PROBABILISTIC PACKET MARKING FOR LARGE-SCALE IP TRACE BACK

ABSTRACT:

An approach to IP traces back based on the probabilistic packet marking paradigm. Our approach, which we call *randomize-and-link*, uses large checksum cords to “link” message fragments in a way that is highly scalable, for the checksums serve both as associative addresses and data integrity verifiers. The main advantage of these checksum cords is that they spread the addresses of possible router messages across a spectrum that is too large for the attacker to easily create messages that collide with legitimate messages.

EXISTING SYSTEM:

The trace back problem is to identify the leaves of , that is, the routers upstream from the victim closest to attack hosts. We model the attacker as an adversary, , who can compromise many hosts and use them as “zombies” in a DDOS attack. We allow that may have knowledge about our trace back algorithms, and that he can even try to design his DDOS attack so as to confuse, break, or delay our algorithms, by “spoofing” the IP headers of attack packets. In this context, we define a DDOS attack to consist of a stream of many attacks packets sent from the attack hosts to the victim (in an attempt to overwhelm the victim). We assume that the attacker cannot compromise routers, however. In so doing, can make it difficult for us to identify some of the routers in the attack tree. In addition, we allow that may know the IP addresses of routers in the Internet; hence, he can try to trick us so as to implicate routers.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



PROPOSED SYSTEM:

The IP trace back problem that are fast and efficient. We prefer solutions that minimize the amount of additional traffic on the Internet needed to solve the trace back problem or create an infrastructure for solving it. Likewise, we want to allow for incremental adoption by routers in any new infrastructure needed for trace back, and we want to minimize the amount of state that must be maintained by routers. That is, if only a subset of routers on the Internet implement our protocol, then we want our trace back algorithm to still work correctly, in this case to identify the leaves of the tree . In addition, the computations needed on the part of the victim to identify the leaves of the attack tree should be fast enough so that can quickly.

In either case, using a 16-bit checksum cord with a two-phase scheme producing a 128-bit message would allow for fast and efficient trace back for attack trees of size up to 2000 routers. In general, our methods do not require that a victim know the topology of the universal tree , we do not require that routers sign any setup messages individually, and we allow for incremental adoption (for the default router action is to process packets in the same way as a nonparticipating router).

2.ON GUARANTEED SMOOTH SWITCHING FOR BUFFERED CROSSBAR SWITCHES**ABSTRACT:**

Scalability considerations drive the evolution of switch design from output queuing to input queuing and further to combined input and cross point queuing (CICQ). However, CICQ switches with credit-based flow control face new challenges of scalability and predictability. In this paper, we propose a novel approach of rate-based smoothed switching, and design a CICQ switch called the smoothed buffered crossbar or sBUX. First, the concept of moothness is developed from two complementary perspectives of covering and spacing, which, commonly known as fairness and jitter, are unified in the same model. Second, a smoothed multiplexer sMUX is designed that allocates bandwidth among competing flows sharing a link and guarantees almost ideal smoothness for each flow. Third, the buffered crossbar sBUX is designed that uses the scheduler sMUX at each input and output, and a two-cell buffer at each crosspoint. It is proved that Sbox guarantees 100% throughput for real-time services and almost ideal smoothness for each flow. Fourth, an on-line bandwidth regulator is designed that periodically estimates bandwidth demand and generates admissible allocations, which enables sBUX to support best-effort services. Simulation shows almost 100% throughput and multi-

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



microsecond average delay. In particular, neither credit-based flow control nor speedup is used, and arbitrary fabric-internal latency is allowed between line cards and the switch core, simplifying the switch implementation.

EXISTING SYSTEM:

NO EXISTING SYSTEM AVAILABLE.

PROPOSED SYSTEM:

Rate-based smoothed switching is the design approach we propose in this paper, which decomposes a switch design into a generic bandwidth regulator and a specific smoothed switch, with an aim to achieve greater scalability and predictability. Rate-based control is in sharp contrast to the predominant approach of credit-based control. The latter uses instantaneous buffer occupancy information at each time slot to compute the schedule and prevent buffer overflow. However, this per-slot computing and communication mode is difficult to scale with faster link speed and larger switch size. The scalability consideration urges us to use more compact information and coarsegrained or batch mode of processing. Rate information is compact in nature as it is applicable for a period of time slots, and can be extracted feasibly in microseconds by our bandwidth regulator. The rate-based smoothed buffered crossbar sBUX removes the credit-based flow control, augments the distributed feature of input and output scheduling, reduces the capacity of each crosspoint buffer to a minimal constant of two cells, and eliminates the need of speedup. All these greatly simplify the implementation and enhance the scalability. Rate-based smoothed switching is also highly predicable. With just a two-cell buffer at each cross point and no speedup, sBUX guarantees 100% throughput for real-time services. In HE *et al.*: ON GUARANTEED SMOOTH SWITCHING FOR BUFFERED CROSSBAR SWITCHES 727 particular, the almost ideal smoothness guarantees imply that rate guarantees are very accurate even in the worst case and in any time window, short or long, finite or infinite.

3.EFFICIENT BROADCASTING USING STORE-MIX- FORWARD METHOD

Abstract:

In later the problem of broadcasting in a wireless network, where all the system of the network are sources that want to transmit information to all other systems. In Some times it directly affects sending data and thus network lifetime. We prove that applying ideas from **network coding** allows realizing significant benefits in terms of energy efficiency for the problem of broadcasting, and proposing very simple algorithms that allow realizing these benefits in

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



practice. In our theoretical analysis shows that **network coding** improves performance by a constant factor in fixed networks. We use distributed algorithms, Network coding can offer improvements of a factor of the number of systems in the network. Finally propose low-complexity distributed algorithm and discuss no of practical systems, and evaluate packet-level simulation.

Existing System:

In the existing system used Conventional Forwarding/Routing Method. In this method sends the data in store-forward multicasting format to one system to another system it will keep on time is 3 transmissions and also it will lose wireless channels, route breakage due to network congestion and also existing system is,

Without network coding

Simple store and forward method send the data to Multicast rate of 1.5 bits per time unit.

so the user attain the time diversity or delay. It can't provide the reliable multicasting to end-to-end. It made a multipath diversity.

Select least number of nodes as forwarders to form a path b/w a Send - Receiver pair and each forwarder transmits each packet once. The problem of broadcasting is interesting not only because it abstracts diverse practical applications, but also because this is a situation where information is mixing in all-all communication. In this method system energy efficiency broadcasting was high. That's why we said affects battery life and thus is a critical design parameter for wireless ad hoc networks.

Proposed System:

In proposed system we used some algorithm to maintain low energy efficiency broadcasting in all-all communication. It's used to improve the performance in data broadcasting Most suitable setting: all too all communications

With network coding

In this method one of the simplest form of data coding

Multicast rate of 2 bits per time unit.

Now you send one data from 1st system to 2nd System and another data from 2nd system to 1st system using 3rd system as a relay. Suppose A and B are not in communication range means it will take 4 transmissions are required to send one data. But in Network coding we needed 3 transmissions.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



Using Practical algorithm Each nodes **sends** out packets obtained as a **random** linear **combination** of packets stored in its buffer. Each node **receives** packets which are a linear combinations of source packets and it **stores** them into buffer.

Advantages:

- Efficiently send data through network
- Send Information for less time consumption
- Without data loss forwarding

4.INCENTIVE-BASED SCHEDULING FOR MARKET-LIKE COMPUTATIONAL GRIDS

Abstract:

In the case of computational grids the consumers and providers share their resources and schedule the decision. And both the parties must have sufficient incentive to play and stay in the market. In this paper we optimize the incentive for both consumers and provides to achieve dual objective. It is to increase the success rate of job execution and to minimize the fairness deviation among resources and in this paper we propose to achieve both this target simultaneously. We present an incentive-based scheduling scheme, which utilizes a peer-to-peer decentralized scheduling framework, a set of local heuristic algorithms, and three market instruments of job announcement, price, and competition degree. This scheme is evaluated by simulation using synthetic and real work groups. The results show that our approach outperforms other scheduling schemes in optimizing incentives for both consumers and providers, leading to highly successful job execution and fair profit allocation.

Existing System:

The existing system is that, many attention have devoted in the area of scheduling redistributed computing, but there were no efficient planning for optimizing incentive to both consumer and provider, utilizing market information.. Many have focused on research for metrics like system utilization, system load balancing and application response time in control grid. But they did not consider market like grid to provide sufficient incentive for participant. However these researches considered only the provider incentive not the consumer incentive.

Proposed System:

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



The main objective of the proposed system is to provide incentive for both consumers and providers. This will intern help both providers and consumers to play a vital roll in market like computational grid. The main advantage of this proposed system is to make the consumers to participate in the process of providing job. The proposed system is design by the following manner.

Consumers and jobs:

Providers and resources:

Incentives for consumers and providers:

5. RATELESS FORWARD ERROR CORRECTION FOR TOPOLOGY-TRANSPARENT SCHEDULING

Abstract:

Topology-transparent scheduling for mobile wireless ad hoc networks has been treated as a theoretical curiosity. This paper makes two contributions towards its practical deployment: 1) We generalize the combinatorial requirement on the schedules and show that the solution is a *cover-free family*. As a result, a much wider number and variety of constructions for schedules exist to match network conditions. 2) In simulation, we closely match the theoretical bound on expected throughput. The bound was derived assuming acknowledgments are available immediately. We use *rateless forward error correction* (RFEC) as an acknowledgment scheme with minimal computational overhead. Since the wireless medium is inherently unreliable, RFEC also offers some measure of automatic adaptation to channel load. These contributions renew interest in topology-transparent scheduling when delay is a principal objective.

Existing System

The existing topology-transparent protocols depend on two parameters: , the number of nodes in the network, and , the maximum node degree. Chlamtac *et al.* gave a construction based on Galois fields and finite geometries using the algebraic property that polynomials of bounded degree cannot have many roots in common; informally, their intersection is small. The schedules derived from the polynomials share the same intersection property and do not overlap in too many slots. In their scheme if a node has at most neighbors, there is at least one collision-free slot to each neighbor within a frame. Their focus was on parameters to minimize schedule length.

Proposed System

In this paper, we make two contributions towards the practical deployment of topology-transparent scheduling: 1) We generalize the combinatorial requirement on topology-transparent schedules and establish that the solution is a well known object called a *cover-free family*. Thus a wealth of combinatorial tools is available for schedule construction. 2) We demonstrate, via simulation for both static and mobile ad hoc networks, that the expected

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



throughput using *rateless forward error correction* (R FEC) closely matches the theoretical bound that assumes immediate feedback availability. Thus unicast can be effectively implemented with low computational overhead. We have established that the combinatorial construction of such schemes can be done much more generally than previously suggested. The combinatorial characterization leads not only to more general construction schemes but also to analytic results suggesting that topology-transparent schemes retain strong throughput and delay performance even when in an environment with neighborhoods larger than anticipated

6. HBA: DISTRIBUTED METADATA MANAGEMENT FOR LARGE CLUSTER-BASED STORAGE SYSTEMS

ABSTRACT : An efficient and distributed scheme for file mapping or file lookup is critical in decentralizing metadata management within a group of metadata servers, here the technique used called **HIERARCHICAL BLOOM FILTER ARRAYS** (HBA) to map filenames to the metadata servers holding their metadata. The Bloom filter arrays with different levels of accuracies are used on each metadata server. The first one with low accuracy and used to capture the destination metadata server information of frequently accessed files. The other array is used to maintain the destination metadata information of all files. Simulation results show our HBA design to be highly effective and efficient in improving the performance and scalability of file systems in clusters with 1,000 to 10,000 nodes (or superclusters) and with the amount of data in the petabyte scale or higher. HBA is reducing metadata operation by using the single metadata architecture instead of 16 metadata server.

Existing System:

File mapping or file lookup is critical in decentralizing metadata management within a group of metadata servers. Following approaches are used in the Existing system.

1. Table-Based Mapping : It fails to balance the load.
2. Hashing-Based Mapping : It has slow directory operations, such as listing the directory contents And renaming directories .
3. Static Tree Partitioning : Cannot balance the load and has a medium lookup time.
4. Dynamic Tree Partitioning : Small memory overhead, incurs a large migration

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



overhead.

Proposed System:

Here we are using the new approaches called HIERARCHICAL BLOOM FILTER ARRAYS (HBA), efficiently route metadata request within a group of metadata servers. There are two arrays used here. First array is used to reduce memory overhead, because it captures only the destination metadata server information of frequently accessed files to keep high management efficiency. And the second one is used to maintain the destination metadata information of all files. Both the arrays are mainly used for fast local lookup.

7.MINIMIZING FILE DOWNLOAD TIME IN STOCHASTIC PEER-TO-PEER NETWORKS

ABSTRACT:

The peer-to-peer (P2P) file-sharing applications are becoming increasingly popular and account for more than 70% of the Internet's bandwidth usage. Measurement studies show that a typical download of a file can take from minutes up to several hours depending on the level of network congestion or the service capacity fluctuation. Here we consider two major factors that have significant impact on average download time, namely, the spatial heterogeneity of service capacities in different source peers and the temporal fluctuation in service capacity of a single source peer. We point out that the common approach of analyzing the average download time based on average service capacity is fundamentally flawed. We rigorously prove that both spatial heterogeneity and temporal correlations in service capacity increase the average download time in P2P networks and then analyze a simple, distributed algorithm to effectively remove these negative factors, thus minimizing the average download time. We show through analysis and simulations that it outperforms most of other algorithms currently used in practice under various network configurations.

Existing System:

The early model for content distribution is a centralized one, in which the service provider simply sets up a server and every user downloads files from it. In this type of network architecture (server-client), many users have to compete for limited resources in terms of bottleneck bandwidth or processing power of a single server. As a result, each user may receive very poor performance. From a single user's perspective, the duration of a download session, or the download time for that individual user is the most often used performance metric. Peer to Peer technology makes the system distributed.

1. Some of the major challenges facing a P2P network in the real world include peer selection, data search and routing.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



2. By reducing actual file transfer time, the download time for each user can be minimized.
3. Nowadays, the common approach for analyze average download time is based on Average Service capacity.

Limitations of Average Service capacity:

4. But it contain two major significant impact
 - a) Spatial Heterogeneity
 - b) Temporal Correlation

Spatial Heterogeneity and Temporal Correlation:

In a P2P network, just like any other network, the service capacities from different source peers are different. There are many reasons for this heterogeneity. On each peer side, physical connection speeds at different peers vary over a wide range. Also, it is reasonable to assume that most peers in a typical P2P network are just personal computers, whose processing powers are also widely different. The limitation in the processing power can limit how fast a peer can service others and hence limits the service capacity.

There are many factors causing this fluctuation. First, the number of connection a source peer allows is changing over time, which creates a fluctuation in the service capacity for each user. Second, some user applications running on a source peer (usually a PC), such as online games, may throttle the CPU and impact the amount of capacity it can offer. Third, temporary congestion at any link in the network can also reduce the service capacity of all users utilizing that link.

PROPOSED SYSTEM:

1. Downloading time can be reduced by using Simple distributed Algorithm with no global Information by using stochastic process.
Here analyze the performance of
 1. Parallel Downloading
 2. Random Chunk Based Switching
 3. Random Time Based Switching
2. Here the impact of stochastic variations of capacities on the average Download time of each peer in the steady state is more rather than in the impact of sources-downloader's dynamics in the transient period.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



8. STATISTICAL TECHNIQUES FOR DETECTING TRAFFIC ANOMALIES THROUGH PACKET HEADER DATA

Abstract:

In this paper we detect the traffic anomalies by monitoring the header data. Some attacks like denial of service led to develop the techniques for identifying the network traffic. If we have the efficient analysis tool we could prevent the network from the traffic before it could get attacked. We can analyze the network traffic with the help of, correlation of the destination IP address in the egress router. The address correlations are data transformed using the discrete wavelet transform for detecting the traffic anomalies. Results from trace-driven evaluation suggest that proposed approach could provide an effective means of detecting anomalies close to the source. We also present a multidimensional indicator using the correlation of port numbers and the number of flows as a means of detecting anomalies.

Existing system:

There is no established existing system to prevent the network traffic. And so we are developing the statically analysis for detecting the traffic anomalies.

Proposed system:

In this project we are going to detect the anomalies using the following three techniques.

- Traffic Analysis at the Source
- General mechanism of detector.
- Trace.

9. A GEOMETRIC APPROACH TO IMPROVING ACTIVE PACKET LOSS MEASUREMENT

Abstract:

This project is fully based on Measurement and estimation of packet loss characteristics. By testing the capability of standard Poisson-modulated end-to-end measurements of loss in a controlled Laboratory environment using IP routers and commodity End hosts. Reporting from the Poisson -modulated probe can be quite inaccurate over the range of traffic conditions. Also here the new algorithm for packet loss measurement that is designed to overcome the deficiencies in Poisson distribution tools. The two geometric distributions are:

- 1) Enable an explicit trade-off between accuracy and impact on the network, and
- 2) Enable more accurate measurements than standard Poisson probing at the

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalsolutions.com



Same rate.

To show the Report about the loss packet called BADABING. And here we show that BADABING reports loss characteristics far more accurately than traditional loss measurement tools.

Existing System:

There are many factors that can contribute to packet loss in the Internet. The most commonly used tools for probing end-to-end paths to measure packet loss resemble the ubiquitous PING utility. In the existing system they are not reported the accurate loss rate of packet. Time consumption very high, Too difficult to study. Evaluated packet loss correlations on longer time scales and developed Markov models for temporal dependence structures. that work reported measures of constancy of loss episode rate, loss episode duration, loss free period duration and Overall loss rates.

Proposed System:

The goal of our study is to understand how to accurately measure loss characteristics on end-to-end paths with probes. We are interested in two specific characteristics of packet loss: loss episode frequency, and loss episode duration [5]. Our study consists of three parts:

(i) Empirical evaluation of the currently prevailing approach, (ii) Development of estimation techniques that are based on novel experimental design, novel probing techniques, and simple validation tests, and (iii) Empirical evaluation of this new methodology.

Our methodology involves dispatching a sequence of probes, each consisting of one or more very closely spaced packets. The aim of a probe is to obtain a snapshot of the state of the network at the instant of probing. As such, the record for each probe indicates whether or not it encountered a loss episode, as evidenced by either the loss or sufficient delay of any of the packets within a probe.

- a) **Loss Episode Frequency Estimation.**
- b) **Loss Episode Duration Estimation**

10.A COST-BASED APPROACH TO ADAPTIVE RESOURCE MANAGEMENT IN DATA STREAM SYSTEMS

Abstract:

DATA stream management systems (DSMSs) have emerged as a new technology to meet the challenging requirements for processing and querying data that arrives continuously in the form of potentially infinite streams from autonomous data sources This paper deals with a novel approach to adaptive resource management for continuous sliding-window queries. This is not the case for sampling-based adaptation techniques. The techniques are compatible with

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



the generally accepted stream semantics and do not collide with query optimizations at runtime, as query results are exact for the selected QoS settings—an advantage compared to load shedding

Existing System:

Existing System is semantics of our adaptation techniques and explained their usage with regard to adaptive memory management. We neither formally nor experimentally presented the impact of those techniques on a query plan

Proposed System:

We introduce two novel techniques for adaptive resource management in a DSMS, namely, adjustments to window sizes and time granularities, along with their QoS constraints. We explain their semantics, suggest syntactical extensions for our query language, and outline their effects on query optimization. .

We develop an appropriate cost model for estimating the resource utilization of continuous sliding window queries. This model is more detailed and extensive than existing ones, as it covers a variety of operators, even aggregation, considers time granularity, and includes reorganization costs caused by the temporal expiration of elements in the operator state due to windowing constructs. .

We describe our adaptive resource management architecture based on our cost model, adaptation techniques, QoS constraints, and a suitable adaptation strategy . .

We conduct thorough experimental studies on synthetic and real-world data streams, based on which we - show that adjustments to window sizes and time granularities are suitable for adaptive resource management,

- validate the accuracy of our cost model,
- illustrate the differences between window reduction and load shedding, and
- prove the scalability of both the techniques and our cost model.

11.WATERMARKING RELATIONAL DATABASE USING OPTIMIZATION BASED TECHNIQUES

Abstract:

For most corporations the volume of sensitive data used by outsourcing providers continues to increase. As the number of different entities having access to a database increases, it gets harder to prevent and trace-back data leakage. We address the problems of proving ownership and unauthorized data distribution (leakage) for relational databases. We propose three techniques that altogether may be used to detect, determine and trace-back

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



data leaks from relational databases. We use business process outsourcing scenarios as the descriptive use case, but our techniques are equally applicable in other use cases when a relational database is shared among many parties and its confidentiality and authenticity needs to be protected. Previous work has shown how to watermark and fingerprint numerical relational data to prove ownership and track unauthorized redistributions respectively. We implemented a proof of concept implementation of our watermarking technique and showed by experimental results that our technique is resilient to tuple deletion, alteration, and insertion attacks.

A **relational database** is a database that groups data using common attributes found in the data set. The resulting "clumps" of organized data are much easier for people to understand. For example, a data set containing all the real estate transactions in a town can be grouped by the year the transaction occurred; or it can be grouped by the sale price of the transaction; or it can be grouped by the buyer's last name; and so on.

Optimization:

Optimization is used to improving the performance. Here we are going to propose data hiding to prove the ownership effectively.

Existing System:

In existing system watermarking is not resilient to tuple deletion, alteration, and insertion attacks.

Proposed system:

In our proposed system we implemented encoding and decoding and data partition technique.

A data set is transformed into a watermarked version by applying a watermark encoding function that also takes as inputs a secret key only known to the copyright owner and a watermark.

Watermark decoding is the process of extracting the embedded watermark using the watermarked data set, the secret keys.

Data partitioning algorithm that partitions the data set based on a secret key. That is if your given correct secret key means watermark text will extract for modification (edit, update, delete).

This tool applies your watermarks to multiple files to protect your copyright. RealWatermark simplifies the process of creating and applying watermark to multiple image files in multiple folders. It supports a mixture of text, copyright symbols, graphic and drawing watermark of any complexity. The multi-level transparency setting allows you to choose and preview how your watermark will affect your image..

Why watermark is datamining?

1. Here we develop data hiding process

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



2. Here text consider as data(tuple)

12.ROUGH SETS-BASED SEARCH ENGINE FOR GRID SERVICE DISCOVERY

Abstract

A **rough set** is a formal approximation of a crisp set (*conventional set*) in terms of a pair of sets which give the *lower* and the *upper* approximation of the original set. The lower and upper approximation sets themselves are crisp sets in the standard version of rough set theory, but in other variations, the approximating sets may be fuzzy sets as well. The computational grid is rapidly evolving into a service-oriented computing infrastructure that facilitates resource sharing and large-scale problem solving over the Internet. Service discovery becomes an issue of vital importance in utilizing grid facilities. This paper presents ROSSE, a Rough sets-based search engine for grid service discovery. Building on the Rough sets theory, ROSSE is novel in its capability to deal with the uncertainty of properties when matching services. In this way, ROSSE can discover the services that are most relevant to a service query from a functional point of view. Since functionally matched services may have distinct nonfunctional properties related to the quality of service (QoS), ROSSE introduces a QoS model to further filter matched services with their QoS values to maximize user satisfaction in service discovery.

Existing System:

In this existing system consumes more time to produces the result. Because it does not have any search engine. Whenever you are asking any query the system search entire data and produces the result. So that it consume more consume. It also makes network traffic and network related problems. In some other systems we have to manually search the entire thing that's what to be want. So it is a very huge thing to do some bid processes.

Proposed System:

In this paper, we have presented ROSSE, a search engine for discovery of grid services. ROSSE builds on the Rough sets theory to dynamically reduce uncertain properties when matching services. In this way, ROSSE increases the accuracy of service discovery. The evaluation results have shown that ROSSE significantly improves the precision and recall compared with UDDI keyword matching and OWL-S matching, respectively. We have also introduced a QoS model to filter functionally matched services with their QoS-related nonfunctional performance. To maximize user satisfaction in service discovery, ROSSE dynamically Determines the set of services that will be presented to users based on the lower and upper approximations of relevant services. We expect to carry out the following work to improve by ROSSE.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



Efficiency: It has been shown that finding a minimal deducts in Rough sets is an NP-hard problem when the number of properties gets large. **Scalability:** The number of services that are registered with ROSSE could be large. Scalability is another issue that needs to be addressed. **Deployment:** Services, once discovered by ROSSE and selected by the user, should be dynamically deployed and invoked.

Ontology alignment: Services may be advertised with properties that follow distinct ontology.

14. HARDWARE ENHANCED ASSOCIATION RULE MINING WITH HASHING AND PIPELINING

Abstarct:

- Data mining techniques have been widely used in various applications. One of the most important data mining applications is association rule mining.
- Apriori-based association rule mining in hardware, one has to load candidate itemsets and a database into the hardware.
- Since the capacity of the hardware architecture is fixed, if the number of candidate itemsets or the number of items in the database is larger than the hardware capacity, the items are loaded into the hardware separately.
- The time complexity of those steps that need to load candidate itemsets or database items into the hardware is in proportion to the number of candidate itemsets multiplied by the number of items in the database. Too many candidate itemsets and a large database would create a performance bottleneck.
- In this paper, we propose a HAsH-based and PiPellned (abbreviated as HAPPI) architecture for hardware enhanced association rule mining. Therefore, we can effectively reduce the frequency of loading the database into the hardware.
- HAPPI solves the bottleneck problem in a priori-based hardware schemes.

Existing System:

- **Apriori** is a classic algorithm for learning association rules. Apriori is designed to operate on database containing transactions. Apriori finds frequent itemsets by scanning a database to check the frequencies of candidate itemsets, which are generated by merging frequent subitemsets. Apriori uses to count candidate item sets efficiently.
- Apriori-based algorithms have undergone bottlenecks because they have too many candidate itemsets. So we can't reduce the frequency of loading the database into the hardware.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



Proposed System:

- We propose a HHash-based and PiPellned (abbreviated as HAPPI) architecture for hardware-enhanced association rule mining.
- There are three hardware modules in our system.
 1. First, when the database is fed into the hardware, the candidate itemsets are compared with the items in the database by the systolic array.
 2. Second, we collect trimming information. From this information, infrequent items in the transactions can be eliminated since they are not useful in generating frequent itemsets through the trimming filter.
 3. Third, we generate itemsets from transactions and hash them into the hash table, which is then used to filter out unnecessary candidate itemsets.
- Our Proposed System solves the bottleneck problem in a priori-based hardware schemes.

15. TRUSTWORTHY COMPUTING UNDER RESOURCE CONSTRAINTS WITH THE DOWN POLICY**Abstract:**

This paper presents a simple way to resolve a complicated network security. It is done by the following two ways. They are as follows, first is the decrypt only when necessary (DOWN) policy, which can substantially improve the ability of low-cost to protect the secrets. The DOWN policy relies on the ability to operate with fractional parts of secrets. This paper discusses the feasibility of extending the DOWN policy to various asymmetric and symmetric cryptographic primitives. The second is cryptographic authentication strategies which employ only symmetric cryptographic primitives, based on novel ID-based key predistribution schemes that demand very low complexity of operations to be performed by the secure coprocessors (ScP) and can take good advantage of the DOWN policy.

Existing System:

In case of the existing system each and every system are considered as a trusted computer. And so the attacker finds it easy to attack the system with fake signals. And also in the emerging network where many are used for some good propos. And in those there a lot of chance for the attacker to send unwanted information. In case of the fire alarm, if all the system are considered as trusted they could send false alarm where it lead to a heavy loss. And so we need a system to protect it. Hence we develop a new system.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



Proposed System:

The proposed system we introduce a new technology to protect the network. This is achieved by the following way. Realizing widespread adoption of such applications Mandates sufficiently trustworthy computers that can be realized at low cost. Apart from facilitating deployment of futuristic applications, the ability to realize trustworthy computers at low cost can also addresses many of the security issues that plague our existing network infrastructure. Although, at first sight, "inexpensive" and "trustworthy" May seem mutually exclusive, a possible strategy is to reduce the complexity of the components inside the trusted boundary. The often heard statement that "complexity is the enemy of security" is far from dogmatic. For one, lower complexity implies better verifiability of compliance. Furthermore, keeping the complexity inside the trust boundary at low levels can obviate the need for proactive measures for heat dissipation. Strategies constrained to simultaneously facilitate shielding and heat dissipation tend to be expensive. On the other hand, unconstrained shielding strategies can be reliable and inexpensive to facilitate.

16.SECURING USER-CONTROLLED ROUTING INFRASTRUCTURES**Abstract:**

In this paper we design an infrastructure for preventing the un trusted parties getting access to the routing information. And also we are achieving flexible and efficient communication. However there are some difficulties in doing so they are the new security vulnerability that is introduced. The flexible control plane of these infrastructures can be exploited to launch many types of powerful attacks with little effort. In this paper, we make several contributions towards studying security issues in forwarding infrastructures (FIs). We present a general model for an FI; analyze potential security vulnerabilities, and present techniques to address these vulnerabilities. The main technique that we introduce in this paper is the use of simple lightweight cryptographic constraints on forwarding entries. We show that it is possible to prevent a large class of Attacks on end-hosts and bound the flooding attacks that can be launched on the infrastructure nodes to a small constant value.

Existing System :

In case of the existing system all the end user and also the third parties are given control over the routing path. As the end users are given control there where many misuse if the routing occurred. And also many new vulnerability have been introduced which made the process of

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



preventing the end users became tedious. And hence there need a research to avoid the third parties in controlling the routing.

Proposed System :

In the system we are going to develop a infrastructure that can prevent the end user in having control over the routing. And also the infrastructure that is developed is the forwarding infrastructure.

17.CREDIT CARD FRAUD DETECTION USING HIDDEN MARKOV MODEL**Abstract:**

Now a day the usage of credit cards has dramatically increased. As credit card becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In this paper, we model the sequence of operations in credit card transaction processing using a Hidden Markov Model (HMM) and show how it can be used for the detection of frauds. An HMM is initially trained with the normal behavior of a cardholder. If an incoming credit card transaction is not accepted by the trained HMM with sufficiently high probability, it is considered to be fraudulent. At the same time, we try to ensure that genuine transactions are not rejected. We present detailed experimental results to show the effectiveness of our approach and compare it with other techniques available in the literature.

Existing System:

In case of the existing system the fraud is detected after the fraud is done that is, the fraud is detected after the complaint of the card holder. And so the card holder faced a lot of trouble before the investigation finish. And also as all the transaction is maintained in a log, we need to maintain a huge data. And also now a days lot of online purchase are made so we don't know the person how is using the card online, we just capture the IP address for verification purpose. So there need a help from the cyber crime to investigate the fraud. To avoid the entire above disadvantage we propose the system to detect the fraud in a best and easy way.

Proposed System:

In proposed system, we present a Hidden Markov Model (HMM).Which does not require fraud signatures and yet is able to detect frauds by considering a cardholder's spending habit. Card transaction processing sequence by the stochastic process of an HMM. The details of items

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com



purchased in Individual transactions are usually not known to an FDS running at the bank that issues credit cards to the cardholders. Hence, we feel that HMM is an ideal choice for addressing this problem. Another important advantage of the HMM-based approach is a drastic reduction in the number of False Positives transactions identified as malicious by an FDS although they are actually genuine. An FDS runs at a credit card issuing bank. Each incoming transaction is submitted to the FDS for verification. FDS receives the card details and the value of purchase to verify, whether the transaction is genuine or not. The types of goods that are bought in that transaction are not known to the FDS. It tries to find any anomaly in the transaction based on the spending profile of the cardholder, shipping address, and billing address, etc.

Advantage

1. The detection of the fraud use of the card is found much faster than the existing system.
2. In case of the existing system even the original card holder is also checked for fraud detection. But in this system no need to check the original user as we maintain a log.
3. The log which is maintained will also be a proof for the bank for the transaction made.
4. We can find the most accurate detection using this technique.
5. This reduces the tedious work of an employee in the bank.

4th floor Oberle Tower Balmatta Mangalore 0824-4261407, 9886271407

raghav@goalitsolutions.com

