

NCCCT

Promise for the Best Projects

**IEEE Transaction Papers
Abstract enclosed**

For Complete Paper, PI contact us

IEEE Papers – 2009, 2008, 2007 and so on

To Search specific year

Use Ctrl + F and specify year

It will give year wise results

e.g – Ctrl + F and mention 2009, you will get 50+ Projects

A FLEXIBLE PRIVACY-ENHANCED LOCATION-BASED SERVICES SYSTEM FRAMEWORK AND PRACTICE

Location-based services (LBSs) are becoming increasingly important to the success and attractiveness of next-generation wireless systems. However, a natural tension arises between the need for user privacy and the flexible use of location information. In this paper, we present a framework to support privacy-enhanced LBSs.

We classify the services according to several basic criteria, And we propose a hierarchical key distribution method to support these services. The main idea behind the system is to hierarchically encrypt location information under different keys, and distribute the appropriate keys only to group members with the necessary permission. Four methods are proposed to deliver hierarchical location information while maintaining privacy.

We propose a key tree-rebalancing algorithm to maintain the rekeying performance of the group key management. Furthermore, we present a practical LBS system implementation. Hierarchical location information coding offers flexible location information access which enables a rich set of LBSs.

Our load tests show such a system is highly practical with good efficiency and scalability.

Index Terms

Location-based services, location privacy, social networks, hierarchical key distribution.

CONTENTION-AWARE PERFORMANCE ANALYSIS OF MOBILITY-ASSISTED ROUTING

A large body of work has theoretically analyzed the performance of mobility-assisted routing schemes for intermittently connected mobile networks. However, the vast majority of these prior studies have ignored wireless contention.

Recent papers have shown through simulations that ignoring contention leads to inaccurate and misleading results, even for sparse networks. In this paper, we analyze the performance of routing schemes under contention.

First, we introduce a mathematical framework to model contention. This framework can be used to analyze any routing scheme with any mobility and channel model. Then, we use this framework to compute the expected delays for different representative mobility-assisted routing schemes under random direction, random waypoint, and community-based mobility models.

Finally, we use these delay expressions to optimize the design of routing schemes while demonstrating that designing and optimizing routing schemes using analytical expressions that ignore contention can lead to sub optimal or even erroneous behavior.

Index Terms

Delay-tolerant networks, wireless contention, performance analysis, mobility-assisted routing.

NODE ISOLATION MODEL AND AGE-BASED NEIGHBOR SELECTION IN UNSTRUCTURED P2P NETWORKS

Previous analytical studies of unstructured P2P resilience have assumed exponential user lifetimes and only considered age-independent neighbor replacement. In this paper, we overcome these limitations by introducing a general node-isolation model for heavy-tailed user lifetimes and arbitrary neighbor-selection algorithms.

Using this model, we analyze two age-biased neighbor-selection strategies and show that they significantly improve the residual lifetimes of chosen users, which dramatically reduces the probability of user isolation and graph partitioning compared with uniform selection of neighbors.

In fact, the second strategy based on random walks on age-proportional graphs demonstrates that, for lifetimes with infinite variance, the system monotonically increases its resilience as its age and size grow.

Specifically, we show that the probability of isolation converges to zero as these two metrics tend to infinity. We finish the paper with simulations in finite-size graphs that demonstrate the effect of this result in practice.

Index Terms

Age-based selection, heavy-tailed lifetimes, node isolation, peer-to-peer networks, user churn.

A NOVEL APPROACH FOR COMPUTATION-EFFICIENT REKEYING FOR MULTICAST KEY DISTRIBUTION

An important problem for secure group communication is key distribution. Most of the centralized group key management schemes employ high rekeying cost.

Here we introduce a novel approach for computation efficient rekeying for multicast key distribution. This approach reduces the rekeying cost by employing a hybrid group key management scheme (involving both centralized and contributory key management schemes).

The group controller uses the MDS Codes, a class of error control codes, to distribute the multicast key dynamically. In order to avoid frequent rekeying as and when the user leaves, a novel approach is introduced where clients recompute the new group key with minimal computation.

This approach ensures forward secrecy as well as backward secrecy and significantly reduces the rekeying cost and communication cost. This scheme well suits wireless applications where portable devices require low computation.

Index Terms

Erasure decoding, Key Distribution, MDS Codes, Multicast.

COLLUSIVE PIRACY PREVENTION IN P2P CONTENT DELIVERY NETWORKS

Collusive piracy is the main source of intellectual property violations within the boundary of a P2P network. Paid clients (colluders) may illegally share copyrighted content files with unpaid clients (pirates). Such online piracy has hindered the use of open P2P networks for commercial content delivery.

We propose a proactive content poisoning scheme to stop colluders and pirates from alleged copyright infringements in P2P file sharing. The basic idea is to detect pirates timely with identity-based signatures and time stamped tokens.

The scheme stops collusive piracy without hurting legitimate P2P clients by targeting poisoning on detected violators, exclusively. We developed a new peer authorization protocol (PAP) to distinguish pirates from legitimate clients. Detected pirates will receive poisoned chunks in their repeated attempts. Pirates are thus severely penalized with no chance to download successfully in tolerable time.

Based on simulation results, we find 99.9 percent prevention rate in Gnutella, KaZaA, and Freenet. We achieved 85- 98 percent prevention rate on eMule, eDonkey, Morpheus, etc. The scheme is shown less effective in protecting some poison-resilient networks like BitTorrent and Azureus. Our work opens up the low-cost P2P technology for copyrighted content delivery.

The advantage lies mainly in minimum delivery cost, higher content availability, and copyright compliance in exploring P2P network resources.

Index Terms

Peer-to-peer networks, content poisoning, copyright protection, network security.

OPPORTUNISTIC SCHEDULING WITH RELIABILITY GUARANTEES IN COGNITIVE RADIO NETWORKS - 2009

We develop opportunistic scheduling policies for cognitive radio networks that maximize the throughput utility of these secondary (unlicensed) users subject to maximum collision constraints with the primary (licensed) users.

We consider a cognitive network with static primary users and potentially mobile secondary users.

We use the technique of Lyapunov Optimization to design an online flow control, scheduling, and resource allocation algorithm that meets the desired objectives and provides explicit performance guarantees.

Index Terms

Cognitive radio, queuing analysis, resource allocation, Lyapunov optimization.

**GENERALIZED SEQUENCE-BASED AND REVERSE
SEQUENCE-BASED MODELS FOR BROADCASTING HOT
VIDEOS – 2009**

It has been well recognized as an efficient approach for broadcasting popular videos by partitioning a video data stream into multiple segments and launching each segment through an individual channel simultaneously and periodically.

Based on the design premises, some recent studies, including skyscraper broadcasting (SkB), client-centric approach (CCA), greedy disk-conserving broadcasting (GDB), and reverse fast broadcasting (RFB) schemes, etc., have been reported. To study the client segment downloading process, this paper first introduces an applicable sequence-based broadcasting model that can be used to minimize the required buffer size.

By extending RFB, this paper further proposes a reverse sequence-based broadcasting model, which can generally improve the existing schemes such as SkB, CCA, GDB, and FB in terms of the relaxed client buffer size.

To have a deeper understanding on the proposed reverse model, the upper bound of the client buffer requirement is obtained through a comprehensive analysis, which is proved to be much smaller than the conventional sequence model by 25% to 50%. Based on the proposed reverse model, a reverse sequence-based broadcasting scheme is developed for achieving smaller delay than CCA and GDB.

Index Terms

Hot-video broadcasting, video-on-demand (VOD), buffers, cable TV.

**CHARMY: A FRAMEWORK FOR DESIGNING AND VERIFYING
ARCHITECTURAL SPECIFICATIONS PATRIZIO PELLICCIONE,
PAOLA INVERARDI, AND HENRY MUCCINI**

Introduced in the early stages of software development, the CHARMY framework assists the software architect in making and evaluating architectural choices. Rarely, the software architecture of a system can be established once and forever.

Most likely poorly defined and understood architectural constraints and requirements force the software architect to accept ambiguities and move forward to the construction of a suboptimal software architecture. CHARMY aims to provide an easy and practical tool for supporting the iterative modeling and evaluation of software architectures. From an UML-based architectural design, an executable prototype is automatically created.

CHARMY simulation and model checking features help in understanding the functioning of the system and discovering potential inconsistencies of the design. When a satisfactory and stable software architecture is reached, Java code conforming to structural software architecture constraints is automatically generated through suitable transformations. The overall approach is tool supported.

Index Terms

Software architectures, model checking.

COMPUTATION-EFFICIENT MULTICAST KEY DISTRIBUTION

Efficient key distribution is an important problem for secure group communications. The communication and storage complexity of multicast key distribution problem has been studied extensively. In this paper, we propose a new multicast key distribution scheme whose computation complexity is significantly reduced.

Instead of using conventional encryption algorithms, the scheme employs MDS codes, a class of error control codes, to distribute multicast key dynamically. This scheme drastically reduces the computation load of each group member compared to existing schemes employing traditional encryption algorithms.

Such a scheme is desirable for many wireless applications where portable devices or sensors need to reduce their computation as much as possible due to battery power limitations. Easily combined with any key-tree-based schemes, this scheme provides much lower computation complexity while maintaining low and balanced communication complexity and storage complexity for secure dynamic multicast key distribution.

Index Terms

Key distribution, multicast, MDS codes, erasure decoding, computation complexity.

AN EFFICIENT CLUSTERING SCHEME TO EXPLOIT HIERARCHICAL DATA IN NETWORK TRAFFIC ANALYSIS

There is significant interest in the data mining and network management communities about the need to improve existing techniques for clustering multivariate network traffic flow records so that we can quickly infer underlying traffic patterns.

In this paper, we investigate the use of clustering techniques to identify interesting traffic patterns from network traffic data in an efficient manner.

We develop a framework to deal with mixed type attributes including numerical, categorical, and hierarchical attributes for a one-pass hierarchical clustering algorithm.

We demonstrate the improved accuracy and efficiency of our approach in comparison to previous work on clustering network traffic.

Index Terms

Traffic analysis, network management, network monitoring, clustering, classification and association rules, hierarchical clustering.

A SURVEY OF LEARNING-BASED TECHNIQUES OF EMAIL SPAM FILTERING - 2008

Email spam is one of the major problems of the today's Internet, bringing financial damage to companies and annoying individual users. Among the approaches developed to stop spam, filtering is an important and popular one.

In this paper we give an overview of the state of the art of machine learning applications for spam filtering, and of the ways of evaluation and comparison of different filtering methods.

We also provide a brief description of other branches of anti-spam protection and discuss the use of various approaches in commercial and noncommercial anti-spam software solutions

BOTMINER: CLUSTERING ANALYSIS OF NETWORK TRAFFIC FOR PROTOCOL- AND STRUCTURE-INDEPENDENT BOTNET DETECTION

Botnets are now the key platform for many Internet attacks, such as spam, distributed denial-of-service (DDoS), identity theft, and phishing. Most of the current botnet detection approaches work only on specific botnet command and control (C&C) protocols (e.g., IRC) and structures (e.g., centralized), and can become ineffective as botnets change their C&C techniques.

In this paper, we present a general detection framework that is independent of botnet C&C protocol and structure, and requires no a priori knowledge of botnets (such as captured bot binaries and hence the botnet signatures, and C&C server names/addresses).

We start from the definition and essential properties of botnets. We define a botnet as a coordinated group of malware instances that are controlled via C&C communication channels. The essential properties of a botnet are that the bots communicate with some C&C servers/peers, perform malicious activities, and do so in a similar or correlated way.

Accordingly, our detection framework clusters similar communication traffic and similar malicious traffic, and performs cross cluster correlation to identify the hosts that share both similar communication patterns and similar malicious activity patterns. These hosts are thus bots in the monitored network.

We have implemented our BotMiner prototype system and evaluated it using many real network traces. The results show that it can detect real-world botnets (IRC-based, HTTP-based, and P2P botnets including Nugache and Storm worm), and has a very low false positive rate.

DUAL-LINK FAILURE RESILIENCY THROUGH BACKUP LINK MUTUAL EXCLUSION

Networks employ link protection to achieve fast recovery from link failures. While the first link failure can be protected using link protection, there are several alternatives for protecting against the second failure.

This paper formally classifies the approaches to dual-link failure resiliency. One of the strategies to recover from dual-link failures is to employ link protection for the two failed links independently, which requires that two links may not use each other in their backup paths if they may fail simultaneously.

Such a requirement is referred to as backup link mutual exclusion (BLME) constraint and the problem of identifying a backup path for every link that satisfies the above requirement is referred to as the BLME problem.

This paper develops the necessary theory to establish the sufficient conditions for existence of a solution to the BLME problem. Solution methodologies for the BLME problem is developed using two approaches by:

- 1) formulating the backup path selection as an integer linear program;
- 2) developing a polynomial time heuristic based on minimum cost path routing.

The ILP formulation and heuristic are applied to six networks and their performance is compared with approaches that assume precise knowledge of dual-link failure. It is observed that a solution exists for all of the six networks considered. The heuristic approach is shown to obtain feasible solutions that are resilient to most dual-link failures, although the backup path lengths may be significantly higher than optimal. In addition, the paper illustrates the significance of the knowledge of failure location by illustrating that network with higher connectivity may require lesser capacity than one with a lower connectivity to recover from dual-link failures.

Index Terms

Backup link mutual exclusion, dual-link failures, link protection, optical networks.

ADAPTIVE NEURAL NETWORK TRACKING CONTROL OF MIMO NONLINEAR SYSTEMS WITH UNKNOWN DEAD ZONES AND CONTROL DIRECTIONS

In this paper, adaptive neural network (NN) tracking control is investigated for a class of uncertain multiple-input-multiple-output (MIMO) nonlinear systems in triangular control structure with unknown nonsymmetric dead zones and control directions.

The design is based on the principle of sliding mode control and the use of Nussbaum-type functions in solving the problem of the completely unknown control directions. It is shown that the dead-zone output can be represented as a simple linear system with a static time-varying gain and bounded disturbance by introducing characteristic function.

By utilizing the integral-type Lyapunov function and introducing an adaptive compensation term for the upper bound of the optimal approximation error and the dead-zone disturbance, the closed-loop control system is proved to be semiglobally uniformly ultimately bounded, with tracking errors converging to zero under the condition that the slopes of unknown dead zones are equal. Simulation results demonstrate the effectiveness of the approach.

Index Terms

Adaptive control, dead zone, neural network (NN) control, Nussbaum function, sliding mode control.

A FRAMEWORK FOR THE CAPACITY EVALUATION OF MULTIHOP WIRELESS NETWORKS, 2009

The specific challenges of multihop wireless networks lead to a strong research effort on efficient protocols design where the offered capacity is a key objective. More specifically, routing strategy largely impacts the network capacity, i.e. the throughput offered to each flow.

In this work, we propose a complete framework to compute the upper and the lower bounds of the network capacity according to a physical topology and a given routing protocol. The radio resource sharing principles of CSMA-CA is modeled as a set of linear constraints with two models of fairness. The first one assumes that nodes have a fair access to the channel, while the second one assumes that on the radio links.

We then develop a pessimistic and an optimistic scenarios for radio resource sharing, yielding a lower bound and an upper bound on the network capacity for each fairness case. Our approach is independent of the network topology and the routing protocols, and provides therefore a relevant framework for their comparison.

We apply our models to a comparative analysis of a well-known flat routing protocol OLSR against two main self-organized structure approaches, VSR and localized CDS.

Index Terms

Network capacity, multihop wireless networks, upper and lower bounds, linear programming

CONTINUOUS FLOW WIRELESS DATA BROADCASTING FOR HIGH-SPEED ENVIRONMENTS

With the increasing popularity of wireless networks and mobile computing, data broadcasting has emerged as an efficient way of delivering data to mobile clients having a high degree of commonality in their demand patterns.

This paper proposes an adaptive wireless push system that operates efficiently in environments characterized by high broadcasting speeds and a-priori unknown client demands for data items.

The proposed system adapts to the demand pattern of the client population in order to reflect the overall popularity of each data item.

We propose a method for feedback collection by the server so that the client population can enjoy a performance increase in proportion to the broadcasting speed used by the server.

Simulation results are presented which reveal satisfactory performance in environments with a-priori unknown client demands and under various high broadcasting speeds.

Index Terms

Adaptive systems, data broadcasting, high-speed, learning automata.

DYNAMIC AND AUTO RESPONSIVE SOLUTION FOR DISTRIBUTED DENIAL-OF-SERVICE ATTACKS DETECTION IN ISP NETWORK, 2009

Denial of service (DoS) attacks and more particularly the distributed ones (DDoS) are one of the latest threat and pose a grave danger to users, organizations and infrastructures of the Internet. Several schemes have been proposed on how to detect some of these attacks, but they suffer from a range of problems, some of them being impractical and others not being effective against these attacks.

This paper reports the design principles and evaluation results of our proposed framework that autonomously detects and accurately characterizes a wide range of flooding DDoS attacks in ISP network. Attacks are detected by the constant monitoring of propagation of abrupt traffic changes inside ISP network.

For this, a newly designed flow-volume based approach (FVBA) is used to construct profile of the traffic normally seen in the network, and identify anomalies whenever traffic goes out of profile. Consideration of varying tolerance factors make proposed detection system scalable to the varying network conditions and attack loads in real time.

Six-sigma method is used to identify threshold values accurately for malicious flows characterization. FVBA has been extensively evaluated in a controlled test-bed environment. Detection thresholds and efficiency is justified using receiver operating characteristics (ROC) curve.

For validation, KDD 99, a publicly available benchmark dataset is used. The results show that our proposed system gives a drastic improvement in terms of detection and false alarm rate.

Index Terms

Distributed Denial of Service Attacks, False Positives, False Negatives, ISP Network, Network Security

Efficient Multi-Party Digital Signature using Adaptive Secret Sharing for Low-Power Devices in Wireless Networks

In this paper, we propose an efficient multi-party signature scheme for wireless networks where a given number of signees can jointly sign a document, and it can be verified by any entity who possesses the certified group public key.

Our scheme is based on an efficient threshold key generation scheme which is able to defend against both static and adaptive adversaries. Specifically, our key generation method employs the bit commitment technique to achieve efficiency in key generation and share refreshing; our share refreshing method provides proactive protection to long-lasting secret and allows a new signee to join a signing group.

We demonstrate that previous known approaches are not efficient in wireless networks, and the proposed multi-party signature scheme is exible, efficient, and achieves strong security for low-power devices in wireless networks.

Index Terms

Multi-party signature, distributed key generation, elliptic curve cryptosystems.

GUARANTEED DELIVERY FOR GEOGRAPHICAL ANYCASTING IN WIRELESS MULTI-SINK SENSOR AND SENSOR-ACTOR NETWORKS

In the anycasting problem, a sensor wants to report event information to one of sinks or actors. We describe the first localized anycasting algorithms that guarantee delivery for connected multi-sink sensor-actor networks.

Let $S(x)$ be the closest actor/sink to sensor x , and $|xS(x)|$ be distance between them. In greedy phase, a node s forwards the packet to its neighbor v that minimizes the ratio of cost $\text{cost}(|sv|)$ of sending packet to v (here we specifically apply hop-count and power consumption metrics) over the reduction in distance $(|sS(s)| - |vS(v)|)$ to the closest actor/sink.

A variant is to forward to the first neighbor on the shortest weighted path toward v . If none of neighbors reduces that distance then recovery mode is invoked. It is done by face traversal toward the nearest connected actor/sink, where edges are replaced by paths optimizing given cost.

A hop count based and two variants of localized power aware anycasting algorithms are described. We prove guaranteed delivery property analytically and experimentally

HIERARCHICAL BAYESIAN SPARSE IMAGE RECONSTRUCTION WITH APPLICATION TO MRFM

This paper presents a hierarchical Bayesian model to reconstruct sparse images when the observations are obtained from linear transformations and corrupted by an additive white Gaussian noise.

Our hierarchical Bayes model is well suited to such naturally sparse image applications as it seamlessly accounts for properties such as sparsity and positivity of the image via appropriate Bayes priors. We propose a prior that is based on a weighted mixture of a positive exponential distribution and a mass at zero.

The prior has hyperparameters that are tuned automatically by marginalization over the hierarchical Bayesian model. To overcome the complexity of the posterior distribution, a Gibbs sampling strategy is proposed. The Gibbs samples can be used to estimate the image to be recovered, e.g. by maximizing the estimated posterior distribution.

In our fully Bayesian approach the posteriors of all the parameters are available. Thus our algorithm provides more information than other previously proposed sparse reconstruction methods that only give a point estimate.

The performance of the proposed hierarchical Bayesian sparse reconstruction method is illustrated on synthetic data and real data collected from a tobacco virus sample using a prototype MRFM instrument.

Index Terms

Deconvolution, MRFM imaging, sparse representation, Bayesian inference, MCMC methods

OFFLINE LOOP INVESTIGATION FOR HANDWRITING ANALYSIS

Study of Rough Set and Clustering Algorithm in Network Security Management Getting a better grasp of computer network security is of great significance to protect the normal operation of network system.

Based on rough set (RS), clustering model, security features reduction and clustering algorithm are presented, which provides a basis of network security strategies. Further research is to mine and process the dynamic risks and management of network security. Using the reduction methods, the simplified network security assessment data set is established.

The extraction by the decision-making rules is proposed and verified. Through the results, it is concluded that the method could be in line with the actual situation of decision-making rules.

Keywords

RS, clustering algorithm, network security, K-W method

HIGH PERFORMANCE COOPERATIVE TRANSMISSION PROTOCOLS BASED ON MULTIUSER DETECTION AND NETWORK CODING

Cooperative transmission is an emerging communication technique that takes advantage of the broadcast nature of wireless channels. However, due to low spectral efficiency and the requirement of orthogonal channels, its potential for use in future wireless networks is limited.

In this paper, by making use of multi-user detection (MUD) and network coding, cooperative transmission protocols with high spectral efficiency, diversity order, and coding gain are developed.

Compared with the traditional cooperative transmission protocols with single user detection, in which the diversity gain is only for one source user, the proposed MUD cooperative transmission protocols have the merit that the improvement of one user's link can also benefit the other users.

In addition, using MUD at the relay provides an environment in which network coding can be employed. The coding gain and high diversity order can be obtained by fully utilizing the link between the relay and the destination.

From the analysis and simulation results, it is seen that the proposed protocols achieve higher diversity gain, better asymptotic efficiency, and lower bit error rate, compared to traditional MUD schemes and to existing cooperative transmission protocols.

From the simulation results, the performance of the proposed scheme is near optimal as the performance gap is 0.12dB for average bit error rate (BER) 10^{-6} and 1.04dB for average BER 10^{-3} , compared to two performance upper bounds.

Index Terms

Detection, coding, communication networks, and cooperative systems.

NOVEL PACKET-LEVEL RESOURCE ALLOCATION WITH EFFECTIVE QoS PROVISIONING FOR WIRELESS MESH NETWORKS

Joint power-subcarrier-time resource allocation is imperative for wireless mesh networks due to the necessity of packet scheduling for quality-of-service (QoS) provisioning, multi-channel communications, and opportunistic power allocation.

In this work, we propose an efficient intra-cluster packet-level resource allocation approach. Our approach takes power allocation, subcarrier allocation, packet scheduling, and QoS support into account.

The proposed approach combines the merits of a Karush-Kuhn-Tucker (KKT)-driven approach and a genetic algorithm (GA)-based approach.

It is shown to achieve a desired balance between time complexity and system performance. Bounds for the throughputs obtained by real-time and non-real-time traffic are also derived analytically.

Index Terms

Genetic algorithm (GA), Karush-Kuhn-Tucker (KKT), quality-of-service (QoS) provisioning, resource allocation, wireless mesh network (WMN).

MULTI-SERVICE LOAD SHARING FOR RESOURCE MANAGEMENT IN THE CELLULAR/WLAN INTEGRATED NETWORK

With the interworking between a cellular network and wireless local area networks (WLANs), an essential aspect of resource management is taking advantage of the overlay network structure to efficiently share the multi-service traffic load between the interworked systems.

In this study, we propose a new load sharing scheme for voice and elastic data services in a cellular/WLAN integrated network. Admission control and dynamic vertical handoff are applied to pool the free bandwidths of the two systems to effectively serve elastic data traffic and improve the multiplexing gain.

To further combat the cell bandwidth limitation, data calls in the cell are served under an efficient service discipline, referred to as shortest remaining processing time (SRPT) [1]. The SRPT can well exploit the heavy-tailedness of data call size to improve the resource utilization.

An accurate analytical model is developed to determine an appropriate size threshold so that data calls are properly distributed to the integrated cell and WLAN, taking into account the load conditions and traffic characteristics.

It is observed from extensive simulation and numerical analysis that the new scheme significantly improves the overall system performance.

Index Terms

Cellular/WLAN interworking, resource management, quality of service, load sharing, vertical handoff, admission control.

SOBIE:A NOVEL SUPER-NODE P2P OVERLAY BASED ON INFORMATION EXCHANGE

In order to guarantee both the efficiency and robustness in the Peer-to-Peer (P2P) network, the paper designs a novel Super-node Overlay Based on Information Exchange called SOBIE.

Differing from current structured and unstructured, or meshed and tree-like P2P overlay, the SOBIE is a whole new structure to improve the efficiency of searching in the P2P network.

The main contributions are

- 1) to select the super-nodes by considering the aggregation of not only the delay, distance, but also the information exchange frequency, exchange time and query similarity especially;
- 2) to set a score mechanism to identify and prevent the free-riders. Meanwhile, the SOBIE also guarantees the matching between the physical network and logical network and has small-world characteristic to improve the efficiency.

Large number of experiment results show the advantages of the SOBIE including high efficiency and robustness by such different factors as the query success rate, the average query hops, the total number of query messages, the coverage rate and system connectivity.

Index Terms

P2P overlay, super node, information exchange, topology matching, free-riding

OPTIMAL BACKPRESSURE ROUTING FOR WIRELESS NETWORKS WITH MULTI-RECEIVER DIVERSITY

We consider the problem of optimal scheduling and routing in an ad-hoc wireless network with multiple traffic streams and time varying channel reliability.

Each packet transmission can be overheard by a subset of receiver nodes, with a transmission success probability that may vary from receiver to receiver and may also vary with time. We develop a simple backpressure routing algorithm that maximizes network throughput and expends an average power that can be pushed arbitrarily close to the minimum average power required for network stability, with a corresponding tradeoff in network delay.

When channels are orthogonal, the algorithm can be implemented in a distributed manner using only local link error probability information, and supports a “blind transmission” mode (where error probabilities are not required) in special cases when the power metric is neglected and when there is only a single destination for all traffic streams.

For networks with general inter-channel interference, we present a distributed algorithm with constant-factor optimality guarantees.

Index Terms

Broadcast advantage, distributed algorithms, dynamic control, mobility, queueing analysis, scheduling

RANDOMCAST: AN ENERGY-EFFICIENT COMMUNICATION SCHEME FOR MOBILE AD HOC NETWORKS

In mobile ad hoc networks (MANETs), every node overhears every data transmission occurring in its vicinity and thus, consumes energy unnecessarily. In IEEE 802.11 Power Saving Mechanism (PSM), a packet must be advertised before it is actually transmitted.

When a node receives an advertised packet that is not destined to itself, it switches to a low-power sleep state during the data transmission period, and thus, avoids overhearing and conserves energy. However, since some MANET routing protocols such as Dynamic Source Routing (DSR) collect route information via overhearing, they would suffer if they are used in combination with 802.11 PSM.

Allowing no overhearing may critically deteriorate the performance of the underlying routing protocol, while unconditional overhearing may offset the advantage of using PSM. This paper proposes a new communication mechanism, called RandomCast, via which a sender can specify the desired level of overhearing, making a prudent balance between energy and routing performance.

In addition, it reduces redundant rebroadcasts for a broadcast packet, and thus, saves more energy. Extensive simulation using ns-2 shows that RandomCast is highly energy-efficient compared to conventional 802.11 as well as 802.11 PSM-based schemes, in terms of total energy consumption, energy goodput, and energy balance.

Index Terms

Energy balance, energy efficiency, mobile ad hoc networks, network lifetime, overhearing, power saving mechanism.

ADAPTIVE FUZZY FILTERING FOR ARTIFACT REDUCTION IN COMPRESSED IMAGES AND VIDEOS

A fuzzy filter adaptive to both sample's activity and the relative position between samples is proposed to reduce the artifacts in compressed multidimensional signals.

For JPEG images, the fuzzy spatial filter is based on the directional characteristics of ringing artifacts along the strong edges. For compressed video sequences, the motion compensated spatiotemporal filter (MCSTF) is applied to intraframe and interframe pixels to deal with both spatial and temporal artifacts.

A new metric which considers the tracking characteristic of human eyes is proposed to evaluate the flickering artifacts.

Simulations on compressed images and videos show improvement in artifact reduction of the proposed adaptive fuzzy filter over other conventional spatial or temporal filtering approaches.

Index Terms

Artifact reduction, flickering metric, fuzzy filter, motion compensated spatio-temporal filter.

A NEW RELIABLE BROADCASTING IN MOBILE AD HOC NETWORKS

A New Reliable Broadcasting Algorithm for mobile ad hoc networks will guarantee to deliver the messages from different sources to all the nodes of the network.

The nodes are mobile and can move from one place to another. The solution does not require the nodes to know the network size, its diameter and number of nodes in the network. The only information a node has its identity (IP Address) and its position.

On average, only a subset of nodes transmits and they transmit only once to achieve reliable broadcasting. The algorithm will calculate the relative position of the nodes with respect to the broadcasting source node.

The nodes that are farthest from the source node will rebroadcast and this will minimize the number of rebroadcasts made by the intermediate nodes and will reduce the delay latency.

The proposed algorithm will adapt itself dynamically to the number of concurrent broadcasts and will give the least finish time for any particular broadcast. It will be contention free, energy efficient and collision free.

Key words

Broadcasting Algorithm, IP Address, Mobile Ad Hoc Networks, Collision, Delay latency.

AN XML-BASED ADL FRAMEWORK FOR AUTOMATIC GENERATION OF MULTITHREADED COMPUTER ARCHITECTURE SIMULATORS

Computer architecture simulation has always played a pivotal role in continuous innovation of computers. However, constructing or modifying a high quality simulator is time consuming and error-prone.

Thus, often Architecture Description Languages (ADLs) are used to provide an abstraction layer for describing the computer architecture and automatically generating corresponding simulators.

Along the line of such research, we present a novel XML-based ADL, its compiler, and a generation methodology to automatically generate multithreaded simulators for computer architecture. We utilize the industry-standard extensible markup language XML to describe the functionality and architecture of a modeled processor.

Our ADL framework allows users to easily and quickly modify the structure, register set, and execution of a modeled processor. To prove its validity, we have generated several multithreaded simulators with different configurations based on the MIPS five-stage processor, and successfully tested with two programs.

CLONE DETECTION AND REMOVAL FOR ERLANG/OTP WITHIN A REFACTORING ENVIRONMENT

A well-known bad code smell in refactoring and software maintenance is duplicated code, or code clones. A code clone is a code fragment that is identical or similar to another.

Unjustified code clones increase code size, make maintenance and comprehension more difficult, and also indicate design problems such as lack of encapsulation or abstraction.

This paper proposes a token and AST based hybrid approach to automatically detecting code clones in Erlang/OTP programs, underlying a collection of refactorings to support user-controlled automatic clone removal, and examines their application in substantial case studies.

Both the clone detector and the refactorings are integrated within Wrangler, the refactoring tool developed at Kent for Erlang/OTP

Keywords

Erlang, refactoring, Wrangler, duplicated code, program analysis, program transformation.

A RELATION-BASED PAGE RANK ALGORITHM FOR SEMANTIC WEB SEARCH ENGINES

With the tremendous growth of information available to end users through the Web, search engines come to play ever a more critical role. Nevertheless, because of their general-purpose approach, it is always less uncommon that obtained result sets provide a burden of useless pages.

The next-generation Web architecture, represented by the Semantic Web, provides the layered architecture possibly allowing overcoming this limitation.

Several search engines have been proposed, which allow increasing information retrieval accuracy by exploiting a key content of Semantic Web resources, that is, relations. However, in order to rank results, most of the existing solutions need to work on the whole annotated knowledge base.

In this paper, we propose a relation-based page rank algorithm to be used in conjunction with Semantic Web search engines that simply relies on information that could be extracted from user queries and on annotated resources.

Relevance is measured as the probability that a retrieved resource actually contains those relations whose existence was assumed by the user at the time of query definition.

Index Terms

Semantic Web, knowledge retrieval, search process, query formulation.

EFFICIENT AND SECURE CONTENT PROCESSING AND DISTRIBUTION BY COOPERATIVE INTERMEDIARIES

Content services such as content filtering and transcoding adapt contents to meet system requirements, display capacities, or user preferences.

Data security in such a framework is an important problem and crucial for many Web applications. In this paper, we propose an approach that addresses data integrity and confidentiality in content adaptation and caching by intermediaries.

Our approach permits multiple intermediaries to simultaneously perform content services on different portions of the 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.

Index Terms

Data sharing, distributed systems, integrity, security.

HIGH MULTIPLICITY SCHEDULING OF FILE TRANSFERS WITH DIVISIBLE SIZES MULTIPLE CLASSES OF PATHS - DEC 2008

Distributed applications and services requiring the transfer of large amounts of data have been developed and deployed world wide.

The best effort model of the Internet cannot provide these applications with the so much needed quality of service guarantees, making necessary the development of file transfer scheduling techniques, which optimize the usage of network resources.

In this paper we consider the high multiplicity scheduling of file transfers over multiple classes of paths with the objective of minimizing the makespan, when the files have divisible sizes.

We also consider another objective, that of maximizing the total profit, in the context of some special types of mutual exclusion constraints (tree and clique constraint graphs).

Index Terms

file transfer scheduling, divisible sizes, high multiplicity, makespan minimization, greedy, binary search, mutual exclusion, tree, clique, dynamic programming.

ENHANCED COMMUNAL GLOBAL, LOCAL MEMORY MANAGEMENT FOR EFFECTIVE PERFORMANCE OF CLUSTER COMPUTING

Memory management becomes a prerequisite when handling applications that require immense volume of data in Cluster Computing.

For example when executing data pertaining to satellite images for remote sensing or defense purposes, scientific or engineering applications. Here even if the other factors perform to the maximum possible levels and if memory management is not properly handled the performance will have a proportional degradation.

Hence it is critical to have a fine memory management technique deployed to handle the stated scenarios. To overwhelm the stated problem we have extended our previous work with a new technique that manages the data in Global Memory and Local Memory and enhances the performance of communicating across clusters for data access.

The issue of the Global Memory and Local Memory Management is solved with the approach discussed in this paper.

Experimental results show performance improvement to considerable levels with the implementation of the concept, specifically when the cost of data access from other clusters is higher and is proportionate to the amount of data.

Keywords:

High Performance Cluster Computing, Job Scheduling, Global Memory Management, Local Memory Management

PEERTALK: A PEER-TO-PEER MULTI-PARTY VOICE-OVER-IP SYSTEM

Multi-party voice-over-IP (MVoIP) services allow a group of people to freely communicate with each other via Internet, which have many important applications such as on-line gaming and teleconferencing. In this paper, we present a peer-to-peer MVoIP system called peerTalk.

Compared to traditional approaches such as server-based mixing, peerTalk achieves better scalability and failure resilience by dynamically distributing stream processing workload among different peers.

Particularly, peerTalk decouples the MVoIP service delivery into two phases: mixing phase and distribution phase. The decoupled model allows us to explore the asymmetric property of MVoIP services (e.g., distinct speaking/listening activities, unequal inbound/ out-bound bandwidths) so that the system can better adapt to distinct stream mixing and distribution requirements.

To overcome arbitrary peer departures/failures, peerTalk provides light-weight backup schemes to achieve fast failure recovery. We have implemented a prototype of the peerTalk system and evaluated its performance using both large-scale simulation testbed and real Internet environment. Our initial implementation demonstrates the feasibility of our approach and shows promising results: peerTalk can outperform existing approaches such as P2P overlay multicast and coupled distributed processing for providing MVoIP services.

Index Terms

Peer-to-Peer Streaming, Voice-Over-IP, Adaptive System, Service Overlay Network, Quality-of-Service, Failure Resilience

Probabilistic Group Nearest Neighbor Queries in Uncertain Databases

The importance of query processing over uncertain data has recently arisen due to its wide usage in many real-world applications. In the context of uncertain databases, previous works have studied many query types such as nearest neighbor query, range query, top-k query, skyline query, and similarity join.

In this paper, we focus on another important query, namely, probabilistic group nearest neighbor (PGNN) query, in the uncertain database, which also has many applications. Specifically, given a set, Q , of query points, a PGNN query retrieves data objects that minimize the aggregate distance (e.g., sum, min, and max) to query set Q .

Due to the inherent uncertainty of data objects, previous techniques to answer group nearest neighbor (GNN) query cannot be directly applied to our PGNN problem.

Motivated by this, we propose effective pruning methods, namely, spatial pruning and probabilistic pruning, to reduce the PGNN search space, which can be seamlessly integrated into our PGNN query procedure.

Extensive experiments have demonstrated the efficiency and effectiveness of our proposed approach, in terms of the wall clock time and the speed-up ratio against linear scan.

Index Terms

Probabilistic group nearest neighbor queries, uncertain database

PACKET CACHES ON ROUTERS: THE IMPLICATIONS OF UNIVERSAL REDUNDANT TRAFFIC ELIMINATION

Many past systems have explored how to eliminate redundant transfers from network links and improve network efficiency. Several of these systems operate at the application layer, while the more recent systems operate on individual packets.

A common aspect of these systems is that they apply to localized settings, e.g. at stub network access links. In this paper, we explore the benefits of deploying packet-level redundant content elimination as a universal primitive on all Internet routers. Such a universal deployment would immediately reduce link loads everywhere. However, we argue that far more significant network-wide benefits can be derived by redesigning network routing protocols to leverage the universal deployment.

We develop “redundancy-aware” intra- and inter-domain routing algorithms and show that they enable better traffic engineering, reduce link usage costs, and enhance ISPs’ responsiveness to traffic variations.

In particular, employing redundancy elimination approaches across redundancy-aware routes can lower intra and inter-domain link loads by 10-50%. We also address key challenges that may hinder implementation of redundancy elimination on fast routers. Our current software router implementation can run at OC48 speeds.

Categories and Subject Descriptors: C.2.2 [Computer Communication Networks]: Routing Protocols

General Terms: Algorithms, Design, Measurement.

Keywords: Traffic Redundancy, Routing, Traffic Engineering.

LOCATION-BASED SPATIAL QUERIES WITH DATA SHARING IN WIRELESS BROADCAST ENVIRONMENTS

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 traditional spatial query processing in centralized databases does not address.

For example, a significant challenge is presented by wireless broadcasting environments, which often exhibit high-latency database access. In this paper, we present a novel query processing technique that, while maintaining high scalability and accuracy, manages to reduce the latency considerably in answering location-based spatial queries.

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 illustrate the appeal of our technique through extensive simulation results.

INCREASING PACKET DELIVERY IN AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

Broadcasting in the route discovery and the route maintenance of Ad hoc On-demand Distance Vector (AODV) Routing Protocol provokes a high number of unsuccessful packets deliveries from the source nodes to the destination nodes.

Studies have been undertaken to optimize the rebroadcast focused on the route discovery of the AODV. In this study, lifetime ratio (LR) of the active route for the intermediate node is introduced to increase the number of unsuccessful packets delivery.

Simulation results focused on the improvement of the packet delivery in the routing protocol compared to standard AODV.

The performance metrics are measured by varying the number of nodes and the speeds. The OMNET++ is used to simulate the performance of the metrics.

PROTECTION OF DATABASE SECURITY VIA COLLABORATIVE INFERENCE DETECTION

Malicious users can exploit the correlation among data to infer sensitive information from a series of seemingly innocuous data accesses. Thus, we develop an inference violation detection system to protect sensitive data content.

Based on data dependency, database schema and semantic knowledge, we constructed a semantic inference model (SIM) that represents the possible inference channels from any attribute to the pre-assigned sensitive attributes. The SIM is then instantiated to a semantic inference graph (SIG) for query-time inference violation detection.

For a single user case, when a user poses a query, the detection system will examine his/her past query log and calculate the probability of inferring sensitive information. The query request will be denied if the inference probability exceeds the pre-specified threshold. For multi-user cases, the users may share their query answers to increase the inference probability.

Therefore, we develop a model to evaluate collaborative inference based on the query sequences of collaborators and their task-sensitive collaboration levels. Experimental studies reveal that information authoritativeness and communication fidelity are two key factors that affect the level of achievable collaboration.

An example is given to illustrate the use of the proposed technique to prevent multiple collaborative users from deriving sensitive information via inference.

THE SERVER REASSIGNMENT PROBLEM FOR LOAD BALANCING IN STRUCTURED P2P SYSTEMS

Application-layer peer-to-peer (P2P) networks are considered to be the most important development for next-generation Internet infrastructure. For these systems to be effective, load balancing among the peers is critical.

Most structured P2P systems rely on ID-space partitioning schemes to solve the load imbalance problem and have been known to result in an imbalance factor of in the zone sizes. This paper makes two contributions.

First, we propose addressing the virtual-server-based load balancing problem systematically using an optimization-based approach and derive an effective algorithm to rearrange loads among the peers.

We demonstrate the superior performance of our proposal in general and its advantages over previous strategies in particular. We also explore other important issues vital to the performance in the virtual server framework, such as the effect of the number of directories employed in the system and the performance ramification of user registration strategies.

Second, and perhaps more significantly, we systematically characterize the effect of heterogeneity on load balancing algorithm performance and the conditions in which heterogeneity may be easy or hard to deal with based on an extensive study of a wide spectrum of load and capacity scenarios.

Index Terms

Distributed hash table, load balance, local search, structured peer-to-peer system, generalized assignment

A TREE-BASED PEER-TO-PEER NETWORK WITH QUALITY GUARANTEES

Abstract—Peer-to-peer (P2P) networks often demand scalability, low communication latency among nodes, and low systemwide overhead. For scalability, a node maintains partial states of a P2P network and connects to a few nodes.

For fast communication, a P2P network intends to reduce the communication latency between any two nodes as much as possible. With regard to a low systemwide overhead, a P2P network minimizes its traffic in maintaining its performance efficiency and functional correctness.

In this paper, we present a novel tree-based P2P network with low communication delay and low systemwide overhead. The merits of our tree-based network include

- 1) a tree-shaped P2P network, which guarantees that the degree of a node is constant in probability, regardless of the system size (the network diameter in our tree-based network increases logarithmically with an increase in the system size, and in particular, given a physical network with a power-law latency expansion property, we show that the diameter of our tree network is constant),
and
- 2) provable performance guarantees. We evaluate our proposal by a rigorous performance analysis, and we validate this by extensive simulations.

Index Terms

Peer-to-peer systems, tree-based networks, multicast, performance analysis.

DISTRIBUTED SUFFIX TREE OVERLAY FOR PEER-TO-PEER SEARCH

Establishing an appropriate semantic overlay on peer-to-peer (P2P) networks to obtain both semantic ability and scalability is a challenge. Current DHT-based P2P networks are limited in their ability to support a semantic search.

This paper proposes the Distributed Suffix Tree (DST) overlay as the intermediate layer between the DHT overlay and the semantic overlay to support the search of a keyword sequence. Its time cost is sublinear with the length of the keyword sequence.

Analysis and experiments show that the DST-based search is fast, load-balanced, and useful in realizing an accurate content search on P2P networks.

Index Terms

DHT, knowledge grid, peer-to-peer, semantic overlay, suffix tree, load balance.

EFFICIENT 2-D GRAYSCALE MORPHOLOGICAL TRANSFORMATIONS WITH ARBITRARY FLAT STRUCTURING ELEMENTS

An efficient algorithm is presented for the computation of grayscale morphological operations with arbitrary 2-D flat structuring elements (S.E.). The required computing time is independent of the image content and of the number of gray levels used.

It always outperforms the only existing comparable method, which was proposed in the work by Van Droogenbroeck and Talbot, by a factor between 3.5 and 35.1, depending on the image type and shape of S.E. So far, filtering using multiple S.E.s is always done by performing the operator for each size and shape of the S.E. separately.

With our method, filtering with multiple S.E.s can be performed by a single operator for a slightly reduced computational cost per size or shape, which makes this method more suitable for use in granulometries, dilation-erosion scale spaces, and template matching using the hit-or-miss transform. The discussion focuses on erosions and dilations, from which other transformations can be derived.

Index Terms

Dilation, dilation-erosion scale spaces, erosion, fast algorithm, hit-or-miss transform, mathematical morphology, multiscale analysis.

FUZZY CONTROL MODEL OPTIMIZATION FOR BEHAVIOR-CONSISTENT TRAFFIC ROUTING UNDER INFORMATION PROVISION

This paper presents an H-infinity filtering approach to optimize a fuzzy control model used to determine behavior consistent (BC) information-based control strategies to improve the performance of congested dynamic traffic networks.

By adjusting the associated membership function parameters to better respond to nonlinearities and modeling errors, the approach is able to enhance the computational performance of the fuzzy control model.

Computational efficiency is an important aspect in this problem context, because the information strategies are required in subreal time to be real-time deployable. Experiments are performed to evaluate the effectiveness of the approach.

The results indicate that the optimized fuzzy control model contributes in determining the BC information-based control strategies in significantly less computational time than when the default controller is used.

Hence, the proposed H-infinity approach contributes to the development of an efficient and robust information-based control approach.

Index Terms

Fuzzy control, H-infinity filter, information based control.

RATE ALLOCATION AND NETWORK LIFETIME PROBLEMS FOR WIRELESS SENSOR NETWORKS

An important performance consideration for wireless sensor networks is the amount of information collected by all the nodes in the network over the course of network lifetime. Since the objective of maximizing the sum of rates of all the nodes in the network can lead to a severe bias in rate allocation among the nodes, we advocate the use of lexicographical max-min (LMM) rate allocation.

To calculate the LMM rate allocation vector, we develop a polynomial-time algorithm by exploiting the parametric analysis (PA) technique from linear program (LP), which we call serial LP with Parametric Analysis (SLP-PA).

We show that the SLP-PA can be also employed to address the LMM node lifetime problem much more efficiently than a state-of-the-art algorithm proposed in the literature.

More important, we show that there exists an elegant duality relationship between the LMM rate allocation problem and the LMM node lifetime problem.

Therefore, it is sufficient to solve only one of the two problems. Important insights can be obtained by inferring duality results for the other problem.

Index Terms

Energy constraint, flow routing, lexicographic max-min, linear programming, network capacity, node lifetime, parametric analysis, rate allocation, sensor networks, theory

TOWARDS MULTIMODAL INTERFACES FOR INTRUSION DETECTION

Network intrusion detection has generally been dealt with using sophisticated software and statistical analysis tools. However, occasionally network intrusion detection must be performed manually by administrators, either by detecting the intruders in real-time or by revising network logs, making this a tedious and timeconsuming labor.

To support this, intrusion detection analysis has been carried out using visual, auditory or tactile sensory information in computer interfaces.

However, little is known about how to best integrate the sensory channels for analyzing intrusion detection. We propose a multimodal human-computer interface to analyze malicious attacks during forensic examination of network logs.

We describe a sonification prototype which generates different sounds according to a number of well-known network attacks

STRUCTURE AND TEXTURE FILLING-IN OF MISSING IMAGE BLOCKS IN WIRELESS TRANSMISSION AND COMPRESSION APPLICATIONS

An approach for filling-in blocks of missing data in wireless image transmission is presented in this paper. When compression algorithms such as JPEG are used as part of the wireless transmission process, images are first tiled into blocks of 8 8 pixels.

When such images are transmitted over fading channels, the effects of noise can destroy entire blocks of the image.

Instead of using common retransmission query protocols, we aim to reconstruct the lost data using correlation between the lost block and its neighbors. If the lost block contained structure, it is reconstructed using an image inpainting algorithm, while texture synthesis is used for the textured blocks.

The switch between the two schemes is done in a fully automatic fashion based on the surrounding available blocks.

The performance of this method is tested for various images and combinations of lost blocks. The viability of this method for image compression, in association with lossy JPEG, is also discussed.

Index Terms

Compression, filling-in, inpainting, interpolation, JPEG, restoration, texture synthesis, wireless transmission.

TCP-LP: LOW-PRIORITY SERVICE VIA END-POINT CONGESTION CONTROL

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.

In this paper, 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 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 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) the response times of web connections in the best-effort class decrease by up to 90% when long-lived bulk data transfers use TCP-LP rather than TCP;
- (5) despite their low-priority nature, TCP-LP flows are able to utilize significant amounts of available bandwidth in a wide-area network environment.

Keywords

TCP-LP, TCP, available bandwidth, service prioritization, TCP-transparency.

NETWORK BORDER PATROL: PREVENTING CONGESTION COLLAPSE AND PROMOTING FAIRNESS IN THE INTERNET

The Internet's excellent scalability and robustness result in part from the end-to-end nature of Internet congestion control. End-to-end congestion control algorithms alone, however, are unable to prevent the congestion collapse and unfairness created by applications that are unresponsive to network congestion.

To address these maladies, we propose and investigate a novel congestion avoidance mechanism called Network Border Patrol (NBP). NBP entails the exchange of feedback between routers at the borders of a network in order to detect and restrict unresponsive traffic flows before they enter the network, thereby preventing congestion within the network.

Moreover, NBP is complemented with the proposed enhanced core-stateless fair queueing (ECSFQ) mechanism, which provides fair bandwidth allocations to competing flows.

Both NBP and ECSFQ are compliant with the Internet philosophy of pushing complexity toward the edges of the network whenever possible. Simulation results show that NBP effectively eliminates congestion collapse and that, when combined with ECSFQ, approximately max-min fair bandwidth allocations can be achieved for competing flows.

Keywords:

Internet, congestion control, congestion collapse, max-min fairness, end-to-end argument, corestateless mechanisms, border control

SECURE PASSWORD-BASED PROTOCOL FOR DOWNLOADING A PRIVATE KEY

We present protocols that allow a user Alice, knowing only her name and password, and not carrying a smart card, to “log in to the network” from a “generic” workstation, i.e., one that has all the necessary software installed, but none of the configuration information usually assumed to be known a priori in a security scheme, such as Alice’s public and private keys, her certificate, and the public keys of one or more CAs. By “logging in”, we mean the workstation retrieves this information on behalf of the user.

This would be straightforward if Alice had a cryptographically strong password. We propose protocols that are secure even if Alice’s password is guessable.

We concentrate on the initial retrieval of Alice’s private key from some server Bob on the network. We discuss various protocols for doing this that avoid off-line password guessing attacks by someone eavesdropping or impersonating Alice or Bob.

We discuss auditable vs. unauditable on-line attacks, and present protocols that allow Bob to be stateless, avoid denial-of-service attacks, allow for salt, and are minimal in computation and number of messages.

PROBABILISTIC PACKET MARKING FOR LARGE- SCALE IP TRACEBACK

This paper presents an approach to IP traceback 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.

Index Terms—Associate addresses, checksum cords, distributed denial of service (DDOS), IP, probabilistic packet marking, traceback.

A SIGNATURE-BASED INDEXING METHOD FOR EFFICIENT CONTENT-BASED RETRIEVAL OF RELATIVE TEMPORAL PATTERNS

A number of algorithms have been proposed for the discovery of temporal patterns. 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 paper, we propose a signature-based indexing method to optimize the storage and retrieval of a large collection of relative temporal patterns.

Index Terms

Content-based data mining queries, organizing temporal patterns, signature-based indexing methods.

USING THE CONCEPTUAL COHESION OF CLASSES FOR FAULT PREDICTION IN OBJECT-ORIENTED SYSTEMS

Abstract—High cohesion is a desirable property of software as it positively impacts understanding, reuse, and maintenance. Currently proposed measures for cohesion in Object-Oriented (OO) software reflect particular interpretations of cohesion and capture different aspects of it.

Existing approaches are largely based on using the structural information from the source code, such as attribute references, in methods to measure cohesion. This paper proposes a new measure for the cohesion of classes in OO software systems based on the analysis of the unstructured information embedded in the source code, such as comments and identifiers. The measure, named the Conceptual Cohesion of Classes (C3), is inspired by the mechanisms used to measure textual coherence in cognitive psychology and computational linguistics.

This paper presents the principles and the technology that stand behind the C3 measure. A large case study on three open source software systems is presented which compares the new measure with an extensive set of existing metrics and uses them to construct models that predict software faults.

The case study shows that the novel measure captures different aspects of class cohesion compared to any of the existing cohesion measures. In addition, combining C3 with existing structural cohesion metrics proves to be a better predictor of faulty classes when compared to different combinations of structural cohesion metrics.

Index Terms

Software cohesion, textual coherence, fault prediction, fault proneness, program comprehension, information retrieval, Latent Semantic Indexing.

TCP STARTUP PERFORMANCE IN LARGE BANDWIDTH DELAY NETWORKS

Next generation networks with large bandwidth and long delay pose a major challenge to TCP performance, especially during the startup period.

In this paper we evaluate the performance of TCP Reno/Newreno, Vegas and Hoe's modification in large bandwidth delay networks. We propose a modified Slow-start mechanism, called Adaptive Start (Astart), to improve the startup performance in such networks.

When a connection initially begins or re-starts after a coarse timeout, Astart adaptively and repeatedly resets the Slow-start Threshold (ssthresh) based on an eligible sending rate estimation mechanism proposed in TCP Westwood. By adapting to network conditions during the startup phase, a sender is able to grow the congestion window (cwnd) fast without incurring risk of buffer overflow and multiple losses.

Simulation experiments show that Astart can significantly improve the link utilization under various bandwidth, buffer size and round-trip propagation times. The method avoids both under-utilization due to premature Slowstart termination, as well as multiple losses due to initially setting ssthresh too high, or increasing cwnd too fast.

Experiments also show that Astart achieves good fairness and friendliness toward TCP NewReno. Lab measurements using a FreeBSD Astart implementation are also reported in this paper, providing further evidence of the gains achievable via Astart.

Keywords

congestion control; slow-start; rate estimation, large bandwidth delay networks

DISTRIBUTED DATA MINING IN CREDIT CARD FRAUD DETECTION

CREDIT CARD TRANSACTIONS Continue to grow in number, taking an ever-larger share of the US payment system and leading to a higher rate of stolen account numbers and subsequent losses by banks.

Improved fraud detection thus has become essential to maintain the viability of the US payment system. Banks have used early fraud warning systems for some years.

Large-scale data-mining techniques can improve on the state of the art in commercial practice. Scalable techniques to analyze massive amounts of transaction data that efficiently compute fraud detectors in a timely manner is an important problem, especially for e-commerce.

Besides scalability and efficiency, the fraud-detection task exhibits technical problems that include skewed distributions of training data and nonuniform cost per error, both of which have not been widely studied in the knowledge-discovery and datamining community.

In this article, we survey and evaluate a number of techniques that address these three main issues concurrently. Our proposed methods of combining multiple learned fraud detectors under a “cost model” are general and demonstrably useful; our empirical results demonstrate that we can significantly reduce loss due to fraud through distributed data mining of fraud models.

A SOFTWARE DEFECT REPORT AND TRACKING SYSTEM IN AN INTRANET

This paper describes a case study where SofTrack - a Software Defect Report and Tracking System – was implemented using internet technology in a geographically distributed organization.

Four medium to large size information systems with different levels of maturity are being analyzed within the scope of this project. They belong to the Portuguese Navy's Information Systems Infrastructure and were developed using typical legacy systems technology:

COBOL with embedded SQL for queries in a Relational Database environment. This pilot project of Empirical Software Engineering has allowed the development of techniques to help software managers to better understand, control and ultimately improve the software process.

Among them are the introduction of automatic system documentation, module's complexity assessment and effort estimation for maintenance activities in the organization.

PREDICTIVE JOB SCHEDULING IN A CONNECTION LIMITED SYSTEM USING PARALLEL GENETIC ALGORITHM

Job scheduling is the key feature of any computing environment and the efficiency of computing depends largely on the scheduling technique used. Intelligence is the key factor which is lacking in the job scheduling techniques of today. Genetic algorithms are powerful search techniques based on the mechanisms of natural selection and natural genetics.

Multiple jobs are handled by the scheduler and the resource the job needs are in remote locations. Here we assume that the resource a job needs are in a location and not split over nodes and each node that has a resource runs a fixed number of jobs.

The existing algorithms used are non predictive and employs greedy based algorithms or a variant of it. The efficiency of the job scheduling process would increase if previous experience and the genetic algorithms are used.

In this paper, we propose a model of the scheduling algorithm where the scheduler can learn from previous experiences and an effective job scheduling is achieved as time progresses.

Keywords: Job scheduling, remote resource, Parallel genetic algorithm

AN AGENT BASED INTRUSION DETECTION, RESPONSE AND BLOCKING USING SIGNATURE METHOD IN ACTIVE NETWORKS

As attackers use automated methods to inflict widespread damage on vulnerable systems connected to the network, it has become painfully clear that traditional manual methods of protection do not suffice. This paper discusses an intrusion prevention approach, intrusion detection, response based on active networks that helps to provide rapid response to vulnerability advisories.

A intrusion detection and intrusion blocker that can provide interim protection against a limited and changing set of high-likelihood or high-priority threats. It is expected that this mechanism would be easily and adaptively configured and deployed to keep pace with the ever-evolving threats on the network, intrusion detection and response based on agent system, digital signature used to provide a security.

Active networks are an exciting development in networking services in which the infrastructure provides customizable network services to packets. The custom network services can be deployed by the user inside the packets themselves. In this paper we propose the use of agent based intrusion detection and response. Agents are integrated with the collaborative IDS in order to provide them with a wider array of information to use their response activities.

Keywords: intrusion detection, blocking, response, agents, digital signature.

A NEAR-OPTIMAL MULTICAST SCHEME FOR MOBILE AD HOC NETWORKS USING A HYBRID GENETIC ALGORITHM

Multicast routing is an effective way to communicate among multiple hosts in a network. It outperforms the basic broadcast strategy by sharing resources along general links, while sending information to a set of predefined multiple destinations concurrently.

However, it is vulnerable to component failure in ad hoc network due to the lack of redundancy, multiple paths and multicast tree structure. Tree graph optimization problems (GOP) are usually difficult and time consuming NP-hard or NP-complete problems.

Genetic algorithms (GA) have been proven to be an efficient technique for solving the GOP, in which well-designed chromosomes and appropriate operators are key factors that determine the performance of the GAs.

Limited link, path constraints, and mobility of network hosts make the multicast routing protocol design particularly challenging in wireless ad hoc networks. Encoding trees is a critical scheme in GAs for solving these problems because each code should represent a tree.

Prufer number is the most representative method of vertex encoding, which is a string of $n-2$ integers and can be transformed to an n -node tree. However, genetic algorithm based on Prufer encoding (GAP) does not preserve locality, while changing one element of its vector causes dramatically change in its corresponding tree topology.

In this paper, we propose a novel GA based on sequence and topology encoding (GAST) for multicast protocol is introduced for multicast routing in wireless ad hoc networks and generalizes the GOP of tree-based multicast protocol as well as three associated operators.

It has revealed an efficient method of the reconstruction of multicast tree topology and the experimental results demonstrated the effectiveness of GAST compare to GAP technique

A NOVEL SECURE COMMUNICATION PROTOCOL FOR AD HOC NETWORKS [SCP]

An ad hoc network is a self organized entity with a number of mobile nodes without any centralized access point and also there is a topology control problem which leads to high power consumption and no security, while routing the packets between mobile hosts.

Authentication is one of the important security requirements of a communication network. The common authentication schemes are not applicable in Ad hoc networks.

In this paper, we propose a secure communication protocol for communication between two nodes in ad hoc networks. This is achieved by using clustering techniques. We present a novel secure communication framework for ad hoc networks (SCP); which describes authentication and confidentiality when packets are distributed between hosts with in the cluster and between the clusters.

These cluster head nodes execute administrative functions and network key used for certification. The cluster head nodes (CHs) perform the major operations to achieve our SCP framework with help of Kerberos authentication application and symmetric key cryptography technique, which will be secure, reliable, transparent and scalable and will have less overhead.

Keywords

Security, Authentication, Confidentiality, Clustering.

CONTROLLING IP SPOOFING THROUGH INTERDOMAIN PACKET FILTERS

The Distributed Denial-of-Service (DDoS) attack is a serious threat to the legitimate use of the Internet. Prevention mechanisms are thwarted by the ability of attackers to forge or spoof the source addresses in IP packets. By employing IP spoofing, attackers can evade detection and put a substantial burden on the destination network for policing attack packets.

In this paper, we propose an interdomain packet filter (IDPF) architecture that can mitigate the level of IP spoofing on the Internet. A key feature of our scheme is that it does not require global routing information. IDPFs are constructed from the information implicit in Border Gateway Protocol (BGP) route updates and are deployed in network border routers.

We establish the conditions under which the IDPF framework correctly works in that it does not discard packets with valid source addresses. Based on extensive simulation studies, we show that, even with partial deployment on the Internet, IDPFs can proactively limit the spoofing capability of attackers.

In addition, they can help localize the origin of an attack packet to a small number of candidate networks.

Index Terms

IP spoofing, DDoS, BGP, network-level security and protection, routing protocols

A NEW MODEL FOR SECURE DISSEMINATION OF XML CONTENT

The paper proposes an approach to content dissemination that exploits the structural properties of an Extensible Markup Language (XML) document object model in order to provide an efficient dissemination and at the same time assuring content integrity and confidentiality.

Our approach is based on the notion of encrypted postorder numbers that support the integrity and confidentiality requirements of XML content as well as facilitate efficient identification, extraction, and distribution of selected content portions.

By using such notion, we develop a structurebased routing scheme that prevents information leaks in the XML data dissemination, and assures that content is delivered to users according to the access control policies, that is, policies specifying which users can receive which portions of the contents.

Our proposed dissemination approach further enhances such structurebased, policy-based routing by combining it with multicast in order to achieve high efficiency in terms of bandwidth usage and speed of data delivery, thereby enhancing scalability.

Our dissemination approach thus represents an efficient and secure mechanism for use in applications such as publish–subscribe systems for XML Documents.

The publish–subscribe model restricts the consumer and document source information to the routers to which they register with. Our framework facilitates dissemination of contents with varying degrees of confidentiality and integrity requirements in a mix of trusted and untrusted networks, which is prevalent in current settings across enterprise networks and the web.

Also, it does not require the routers to be aware of any security policy in the sense that the routers do not need to implement any policy related to access control.

Index Terms

Encryption, Extensible Markup Language (XML), postorder traversal, preorder traversal, publish–subscribe, security, structure-based routing, trees

INFRASTRUCTURE OF UNIFIED NETWORK MANAGEMENT SYSTEM DRIVEN BY WEB TECHNOLOGY

As distributed network management systems play an increasingly important role in telecommunication network, the flexible, efficient and low-cost unified NMS infrastructure is a key issue in top-level system design.

We propose a new infrastructure for a Web-driven, distributed unified network management system. The key technologies in practical application are investigated in detail.

The practical application has been implemented using Java and tested on a unified telecommunication network management system.

The experiments and application have demonstrated that the infrastructure is feasible and scalable for operation in current and future telecommunication network management

A/I NET: A NETWORK THAT INTEGRATES ATM AND IP

Future networks need both connectionless and connection-oriented services. IP and ATM are major examples of the two types.

Connectionless IP is more efficient for browsing, e-mail, and other non-real-time services; but for services demanding quality and real-time delivery, connection-oriented ATM is a much better candidate.

Given the popularity of the Internet and the established status of ATM as the broadband transport standard, it is unlikely that one can replace the other.

Therefore, the challenge we face lies in finding an efficient way to integrate the two. This article describes a research project reflecting this trend.

The project aims at efficient integration of the two to eliminate the deficiencies of a standalone ATM or IP network

PERFORMANCE OF A SPECULATIVE TRANSMISSION SCHEME FOR SCHEDULING-LATENCY REDUCTION

Low latency is a critical requirement in some switching applications, specifically in parallel computer interconnection networks. The minimum latency in switches with centralized scheduling comprises two components, namely, the control-path latency and the data-path latency, which in a practical high-capacity, distributed switch implementation can be far greater than the cell duration.

We introduce a speculative transmission scheme to significantly reduce the average control-path latency by allowing cells to proceed without waiting for a grant, under certain conditions.

It operates in conjunction with any centralized matching algorithm to achieve a high maximum utilization and incorporates a reliable delivery mechanism to deal with failed speculations.

An analytical model is presented to investigate the efficiency of the speculative transmission scheme employed in a non-blocking input-queued crossbar switch with receivers per output. Using this model, performance measures such as the mean delay and the rate of successful speculative transmissions are derived.

The results demonstrate that the control-path latency can be almost entirely eliminated for loads up to 50%. Our simulations confirm the analytical results.

Index Terms

Arbiters, electrooptic switches, modeling, packet switching, scheduling.

REDUCING DELAY AND ENHANCING DOS RESISTANCE IN MULTICAST AUTHENTICATION THROUGH MULTIGRADE SECURITY

Many techniques for multicast authentication employ the principle of delayed key disclosure. These methods introduce delay in authentication, employ receiver-side buffers, and are susceptible to denial-of-service (DoS) attacks. Delayed key disclosure schemes have a binary concept of authentication and do not incorporate any notion of partial trust.

This paper introduces staggered timed efficient stream loss-tolerant authentication (TESLA), a method for achieving multigrade authentication in multicast scenarios that reduces the delay needed to filter forged multicast packets and, consequently, mitigates the effects of DoS attacks.

Staggered TESLA involves modifications to the popular multicast authentication scheme, TESLA, by incorporating the notion of multilevel trust through the use of multiple, staggered authentication keys in creating message authentication codes (MACs) for a multicast packet.

We provide guidelines for determining the appropriate buffer size, and show that the use of multiple MACs and, hence, multiple grades of authentication, allows the receiver to flush forged packets quicker than in conventional TESLA.

As a result, staggered TESLA provides an advantage against DoS attacks compared to conventional TESLA. We then examine two new strategies for reducing the time needed for complete authentication.

In the first strategy, the multicast source uses assurance of the trustworthiness of entities in a neighborhood of the source, in conjunction with the multigrade authentication provided by staggered TESLA. The second strategy achieves reduced delay by introducing additional key distributors in the network.

Index Terms

Denial-of-service (DoS) attacks, forge-capable area, message authentication code (MAC), multigrade source authentication, queueing theory, timed efficient stream loss-tolerant authentication (TESLA), trust.

BANDWIDTH EFFICIENT VIDEO MULTICASTING IN MULTIRADIO MULTICELLULAR WIRELESS NETWORKS

In this paper, we propose a new mechanism to select the cells and the wireless technologies for layer-encoded video multicasting in the heterogeneous wireless networks.

Different from the previous mechanisms, each mobile host in our mechanism can select a different cell with a different wireless technology to subscribe each layer of a video stream, and each cell can deliver only a subset of layers of the video stream to reduce the bandwidth consumption.

We formulate the Cell and Technology Selection Problem (CTSP) to multicast each layer of a video stream as an optimization problem. We use Integer Linear Programming to model the problem and show that the problem is NP-hard.

To solve the problem, we propose a distributed algorithm based on Lagrangean relaxation and a protocol based on the proposed algorithm. Our mechanism requires no change of the current video multicasting mechanisms and the current wireless network infrastructures.

Our algorithm is adaptive not only to the change of the subscribers at each layer, but also the change of the locations of each mobile host.

Index Terms

Multicast, layer-encoded video, heterogeneous wireless networks

DISTRIBUTED CACHE UPDATING FOR THE DYNAMIC SOURCE ROUTING PROTOCOL

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. However, heuristics cannot accurately estimate timeouts because topology changes are unpredictable.

In this paper, 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 algorithm does not use any ad hoc parameters, thus making route caches fully adaptive to topology changes.

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.

Index Terms

Mobile ad hoc networks, On-demand routing protocols, Mobility, Distributed cache updating

AN ACKNOWLEDGMENT-BASED APPROACH FOR THE DETECTION OF ROUTING MISBEHAVIOR IN MANETS

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 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.

Index Terms

Mobile Ad Hoc Networks (MANETs), routing misbehavior, node misbehavior, network security, Dynamic Source Routing (DSR).

REDUCING DELAY AND ENHANCING DOS RESISTANCE IN MULTICAST AUTHENTICATION THROUGH MULTIGRADE SECURITY

Many techniques for multicast authentication employ the principle of delayed key disclosure. These methods introduce delay in authentication, employ receiver-side buffers, and are susceptible to denial-of-service (DoS) attacks.

Delayed key disclosure schemes have a binary concept of authentication and do not incorporate any notion of partial trust. This paper introduces staggered timed efficient stream loss-tolerant authentication (TESLA), a method for achieving multigrade authentication in multicast scenarios that reduces the delay needed to filter forged multicast packets and, consequently, mitigates the effects of DoS attacks.

Staggered TESLA involves modifications to the popular multicast authentication scheme, TESLA, by incorporating the notion of multilevel trust through the use of multiple, staggered authentication keys in creating message authentication codes (MACs) for a multicast packet.

We provide guidelines for determining the appropriate buffer size, and show that the use of multiple MACs and, hence, multiple grades of authentication, allows the receiver to flush forged packets quicker than in conventional TESLA. As a result, staggered TESLA provides an advantage against DoS attacks compared to conventional TESLA. We then examine two new strategies for reducing the time needed for complete authentication.

In the first strategy, the multicast source uses assurance of the trustworthiness of entities in a neighborhood of the source, in conjunction with the multigrade authentication provided by staggered TESLA. The second strategy achieves reduced delay by introducing additional key distributors in the network.

Index Terms

Denial-of-service (DoS) attacks, forge-capable area, message authentication code (MAC), multigrade source authentication, queueing theory, timed efficient stream loss-tolerant authentication (TESLA), trust.

A SELF-REPAIRING TREE TOPOLOGY ENABLING CONTENT-BASED ROUTING IN MOBILE AD HOC NETWORKS

Content-based routing (CBR) provides a powerful and flexible foundation for distributed applications. Its communication model, based on implicit addressing, fosters decoupling among the communicating components, therefore meeting the needs of many dynamic scenarios, including mobile ad hoc networks (MANETs).

Unfortunately, the characteristics of the CBR model are only rarely met by available systems, which typically assume that application-level routers are organized in a tree-shaped network with a fixed topology.

In this paper we present COMAN, a protocol to organize the nodes of a MANET in a tree-shaped network able to

- i) selfrepair to tolerate the frequent topological reconfigurations typical of MANETs;**
- ii) achieve this goal through repair strategies that minimize the changes that may impact the CBR layer exploiting the tree. COMAN is implemented and publicly available. Here we report about its performance in simulated scenarios as well as in real-world experiments.**

The results confirm that its characteristics enable reliable and efficient CBR on MANETs.

Index Terms

Content-based routing, publish-subscribe, query-advertise, mobile ad hoc network.

IMAGE TRANSFORMATION USING GRID

The objective of this paper is to design and implement an algorithm to transform an available 2D image into a 3D image. Since the available algorithms are time consuming enhance the efficiency, Grid computing has been used to implement the same.

Grid computing phenomenon can be defined as “A paradigm/infrastructure that enabling the sharing, selection, & aggregation of geographically distributed resources”.

Images captured by devices such as digital camera are generally of two dimensional in nature. But to analyze the images that too in engineering applications the same two-dimensional image if transformed into a three-dimensional image without appreciable data loss will be very useful and effective for analysis.

Conventionally there are some software packages available for converting a 2D image to 3D image. In java graphics API (jdk 1.5) a package for 2D to 3D is there with defined methods for generating algorithms. But when such an algorithm is being designed and developed it was found that it consumed much time for execution.

So a new approach is used here for running such an algorithm over the concept of grid. To illustrate the phenomenon we have developed software which transforms a two dimensional objects to three dimensional objects. In this module, Grid computing has been employed as a platform since it is a rapidly developing field.

Grid computing will be very useful in projects where complexity and time factors are essential. It can also be used effectively to improve the overall system efficiency.

Keywords:

Grid service, Event, Object, Heterogeneity, Data sets, patterns, concept hierarchies, Load distribution

HYBRID INTRUSION DETECTION WITH WEIGHTED SIGNATURE GENERATION OVER ANOMALOUS INTERNET EPISODES

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.

Index Terms

Network security, intrusion detection systems, anomaly detection, signature generation, SNORT and Bro systems, false alarms, Internet episodes, traffic data mining.

PFUSION: A P2P ARCHITECTURE FOR INTERNET-SCALE CONTENT-BASED SEARCH AND RETRIEVAL

The emerging Peer-to-Peer (P2P) model has become a very powerful and attractive paradigm for developing Internet-scale systems for sharing resources, including files and documents.

The distributed nature of these systems, where nodes are typically located across different networks and domains, inherently hinders the efficient retrieval of information.

In this paper, we consider the effects of topologically aware overlay construction techniques on efficient P2P keyword search algorithms. We present the Peer Fusion (pFusion) architecture that aims to efficiently integrate heterogeneous information that is geographically scattered on peers of different networks.

Our approach builds on work in unstructured P2P systems and uses only local knowledge. Our empirical results, using the pFusion middleware architecture and data sets from Akamai's Internet mapping infrastructure (AKAMAI), the Active Measurement Project (NLANR), and the Text REtrieval Conference (TREC) show that the architecture we propose is both efficient and practical.

Index Terms

Information retrieval, peer-to-peer, overlay construction algorithms.

AN ADAPTIVE PROGRAMMING MODEL FOR FAULT-TOLERANT DISTRIBUTED COMPUTING

The capability of dynamically adapting to distinct runtime conditions is an important issue when designing distributed systems where negotiated quality of service (QoS) cannot always be delivered between processes. Providing fault tolerance for such dynamic environments is a challenging task.

Considering such a context, this paper proposes an adaptive programming model for fault-tolerant distributed computing, which provides upper-layer applications with process state information according to the current system synchrony (or QoS).

The underlying system model is hybrid, composed by a synchronous part (where there are time bounds on processing speed and message delay) and an asynchronous part (where there is no time bound). However, such a composition can vary over time, and, in particular, the system may become totally asynchronous (e.g., when the underlying system QoS degrade) or totally synchronous.

Moreover, processes are not required to share the same view of the system synchrony at a given time. To illustrate what can be done in this programming model and how to use it, the consensus problem is taken as a benchmark problem.

This paper also presents an implementation of the model that relies on a negotiated quality of service (QoS) for communication channels.

Index Terms

Adaptability, asynchronous/synchronous distributed system, consensus, distributed computing model, fault tolerance, quality of service.

REDUCING DELAY AND ENHANCING DOS RESISTANCE IN MULTICAST AUTHENTICATION THROUGH MULTIGRADE SECURITY

Many techniques for multicast authentication employ the principle of delayed key disclosure. These methods introduce delay in authentication, employ receiver-side buffers, and are susceptible to denial-of-service (DoS) attacks. Delayed key disclosure schemes have a binary concept of authentication and do not incorporate any notion of partial trust.

This paper introduces staggered timed efficient stream loss-tolerant authentication (TESLA), a method for achieving multigrade authentication in multicast scenarios that reduces the delay needed to filter forged multicast packets and, consequently, mitigates the effects of DoS attacks.

Staggered TESLA involves modifications to the popular multicast authentication scheme, TESLA, by incorporating the notion of multilevel trust through the use of multiple, staggered authentication keys in creating message authentication codes (MACs) for a multicast packet.

We provide guidelines for determining the appropriate buffer size, and show that the use of multiple MACs and, hence, multiple grades of authentication, allows the receiver to flush forged packets quicker than in conventional TESLA.

As a result, staggered TESLA provides an advantage against DoS attacks compared to conventional TESLA. We then examine two new strategies for reducing the time needed for complete authentication. In the first strategy, the multicast source uses assurance of the trustworthiness of entities in a neighborhood of the source, in conjunction with the multigrade authentication provided by staggered TESLA. The second strategy achieves reduced delay by introducing additional key distributors in the network.

Index Terms

Denial-of-service (DoS) attacks, forge-capable area, message authentication code (MAC), multigrade source authentication, queueing theory, timed efficient stream loss-tolerant authentication (TESLA), trust.

BENEFIT-BASED DATA CACHING IN AD HOC NETWORKS

Data caching can significantly improve the efficiency of information access in a wireless ad hoc network by reducing the access latency and bandwidth usage. However, designing efficient distributed caching algorithms is non-trivial when network nodes have limited memory.

In this article, we consider the cache placement problem of minimizing total data access cost in ad hoc networks with multiple data items and nodes with limited memory capacity.

The above optimization problem is known to be NP-hard. Defining benefit as the reduction in total access cost, we present a polynomial-time centralized approximation algorithm that provably delivers a solution whose benefit is at least one-fourth (one-half for uniform-size data items) of the optimal benefit.

The approximation algorithm is amenable to localized distributed implementation, which is shown via simulations to perform close to the approximation algorithm. Our distributed algorithm naturally extends to networks with mobile nodes.

We simulate our distributed algorithm using a network simulator (ns2), and demonstrate that it significantly outperforms another existing caching technique (by Yin and Cao [30]) in all important performance metrics. The performance differential is particularly large in more challenging scenarios, such as higher access frequency and smaller memory.

SCALABLE MULTICASTING IN MOBILE AD HOC NETWORKS

Many potential applications of Mobile Ad hoc Networks (MANETs) involve group communications among the nodes. Multicasting is an useful operation that facilitates group communications. Efficient and scalable multicast routing in MANETs is a difficult issue. In addition to the conventional multicast routing algorithms, recent protocols have adopted the following new approaches: overlays, backbone-based, and stateless. In this paper, we study these approaches from the protocol state management point of view, and compare their scalability behaviors.

To enhance performance and enable scalability, we have proposed a framework for hierarchical multicasting in MANET environments.

Two classes of hierarchical multicasting approaches, termed as domain-based and overlay-based, are proposed. We have considered a variety of approaches that are suitable for different mobility patterns and multicast group sizes. Results obtained through simulations demonstrate enhanced performance and scalability of the proposed techniques.

Index Terms

Hierarchical multicasting, Mobile Ad hoc networks, Domain-based multicasting, Overlay multicasting, Stateless multicasting, Scalability

BUILDING INTELLIGENT SHOPPING ASSISTANTS USING INDIVIDUAL CONSUMER MODELS

This paper describes an Intelligent Shopping Assistant designed for a shopping cart mounted tablet PC that enables individual interactions with customers. We use machine learning algorithms to predict a shopping list for the customer's current trip and present this list on the device.

As they navigate through the store, personalized promotions are presented using consumer models derived from loyalty card data for each individual. In order for shopping assistant devices to be effective, we believe that they have to be powered by algorithms that are tuned for individual customers and can make accurate predictions about an individual's actions.

We formally frame the shopping list prediction as a classification problem, describe the algorithms and methodology behind our system, and show that shopping list prediction can be done with high levels of accuracy, precision, and recall.

Beyond the prediction of shopping lists we briefly introduce other aspects of the shopping assistant project, such as the use of consumer models to select appropriate promotional tactics, and the development of promotion planning simulation tools to enable retailers to plan personalized promotions delivered through such a shopping assistant.

Categories and Subject Descriptors: H.2.8 Database Management Database Applications [Data Mining]

General Terms: Algorithms, Economics, Experimentation.

Keywords: Retail applications, Machine learning, Classification.

APPLICATION OF BPCS STEGANOGRAPHY TO WAVELET COMPRESSED VIDEO

This paper presents a steganography method using lossy compressed video which provides a natural way to send a large amount of secret data. The proposed method is based on wavelet compression for video data and bit-plane complexity segmentation (BPCS) steganography.

In waveletbased video compression methods such as 3-D set partitioning in hierarchical trees (SPIHT) algorithm and Motion- JPEG2000, wavelet coefficients in discrete wavelet transformed video are quantized into a bit-plane structure and therefore BPCS steganography can be applied in the wavelet domain.

3-D SPIHT-BPCS steganography and Motion- JPEG2000-BPCS steganography are presented and tested, which are the integration of 3-D SPIHT video coding and BPCS steganography, and that of Motion-JPEG2000 and BPCS, respectively.

Experimental results show that 3-D SPIHT-BPCS is superior to Motion-JPEG2000-BPCS with regard to embedding performance.

ODAM: AN OPTIMIZED DISTRIBUTED ASSOCIATION RULE MINING ALGORITHM

Association rule mining is an active data mining research area. However, most ARM algorithms cater to a centralized environment. In contrast to previous ARM algorithms, ODAM is a distributed algorithm for geographically distributed data sets that reduces communication costs.

Modern organizations are geographically distributed. Typically, each site locally stores its ever increasing amount of day-to-day data. Using centralized data mining to discover useful patterns in such organizations' data isn't always feasible because merging data sets from different sites into a centralized site incurs huge network communication costs.

Data from these organizations are not only distributed over various locations but also vertically fragmented, making it difficult if not impossible to combine them in a central location. Distributed data mining has thus emerged as an active subarea of data mining research.

A significant area of data mining research is association rule mining. Unfortunately, most ARM algorithms 1-9 focus on a sequential or centralized environment where no external communication is required. Distributed ARM algorithms, on the other hand, aim to generate rules from different data sets spread over various geographical sites; hence, they require external communications throughout the entire process.

DARM algorithms must reduce communication costs so that generating global association rules costs less than combining the participating sites' data sets into a centralized site.

However, most DARM algorithms don't have an efficient message optimization technique, so they exchange numerous messages during the mining process. We have developed a distributed algorithm, called Optimized Distributed Association Mining, for geographically distributed data sets. ODAM generates support counts of candidate itemsets quicker than other DARM algorithms and reduces the size of average transactions, data sets, and message exchanges.

INCREMENTAL SERVICE DEPLOYMENT USING THE HOP BY HOP MULTICAST ROUTING PROTOCOL

IP Multicast is facing a slow take-off although it is a hotly debated topic since more than a decade. Many reasons are responsible for this status. Hence, the Internet is likely to be organized with both unicast and multicast enabled networks.

Thus, it is of utmost importance to design protocols that allow the progressive deployment of the multicast service by supporting unicast clouds. This paper presents HBH (Hop-By- Hop multicast routing protocol).

HBH adopts the source-specific channel abstraction to simplify address allocation and implements data distribution using recursive unicast trees, which allow the transparent support of unicast-only routers.

An important original feature of HBH is its tree construction algorithm that takes into account the unicast routing asymmetries. Since most multicast routing protocols rely on the unicast infrastructure, the unicast asymmetries impact the structure of the multicast trees.

We show through simulation that HBH outperforms other multicast routing protocols in terms of the delay experienced by the receivers and the bandwidth consumption of the multicast trees.

Additionally, we show that HBH can be incrementally deployed and that with a small fraction of HBH-enabled routers in the network HBH outperforms application-layer multicast.

Index Terms

Multicast, routing, service deployment

A DISTRIBUTED DATABASE ARCHITECTURE FOR GLOBAL ROAMING IN NEXT- GENERATION MOBILE NETWORKS

The next-generation mobile network will support terminal mobility, personal mobility, and service provider portability, making global roaming seamless. A location-independent personal telecommunication number (PTN) scheme is conducive to implementing such a global mobile system.

However, the nongeographic PTNs coupled with the anticipated large number of mobile users in future mobile networks may introduce very large centralized databases. This necessitates research into the design and performance of high-throughput database technologies used in mobile systems to ensure that future systems will be able to carry efficiently the anticipated loads.

This paper 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. In addition, two memory-resident database indices, memory-resident direct file and T-tree, are proposed for the location databases to further improve their throughput.

Analysis model and numerical results are presented to evaluate the efficiency of the proposed database architecture.

Results have revealed that the proposed database architecture for location management can effectively support the anticipated high user density in the future mobile networks.

Index Terms

Database architecture, location management, location tracking, mobile networks.

A LOCATION-BASED ROUTING METHOD FOR MOBILE AD HOC NETWORKS

Using location information to help routing is often proposed as a means to achieve scalability in large mobile ad hoc networks. However, location-based routing is difficult when there are holes in the network topology and nodes are mobile or frequently disconnected to save battery. Terminode routing, presented here, addresses these issues.

It uses a combination of location-based routing (Terminode Remote Routing, TRR), used when the destination is far, and link state routing (Terminode Local Routing, TLR), used when the destination is close. TRR uses anchored paths, a list of geographic points (not nodes) used as loose source routing information.

Anchored paths are discovered and managed by sources, using one of two low overhead protocols: Friend Assisted Path Discovery and Geographical Map-based Path Discovery.

Our simulation results show that terminode routing performs well in networks of various sizes. In smaller networks, the performance is comparable to MANET routing protocols.

In larger networks that are not uniformly populated with nodes, terminode routing outperforms existing location-based or MANET routing protocols.

Index Terms

Restricted random waypoint, mobility model, ad hoc network, scalable routing, location-based routing method, robustness to location inaccuracy.

FACE RECOGNITION USING LAPLACIANFACES

We propose an appearance-based face recognition method called the Laplacianface approach. By using Locality Preserving Projections (LPP), the face images are mapped into a face subspace for analysis. Different from Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA) which effectively see only the Euclidean structure of face space, LPP finds an embedding that preserves local information, and obtains a face subspace that best detects the essential face manifold structure.

The Laplacianfaces are the optimal linear approximations to the eigenfunctions of the Laplace Beltrami operator on the face manifold. In this way, the unwanted variations resulting from changes in lighting, facial expression, and pose may be eliminated or reduced.

Theoretical analysis shows that PCA, LDA, and LPP can be obtained from different graph models. We compare the proposed Laplacianface approach with Eigenface and Fisherface methods on three different face data sets. Experimental results suggest that the proposed Laplacianface approach provides a better representation and achieves lower error rates in face recognition.

Index Terms

Face recognition, principal component analysis, linear discriminant analysis, locality preserving projections, face manifold, subspace learning.

SECURE ELECTRONIC DATA INTERCHANGE OVER THE INTERNET

Numerous retailers, manufacturers, and other companies within business supply chains are leveraging Applicability Statement #2 (AS2) and other standards developed by the IETF's Electronic Data Interchange over the Internet (EDI-INT) working group (www.imc.org/ietf-ediint/).

Founded in 1996 to develop a secure transport service for EDI business documents, the EDI-INT WG later expanded its focus to include XML and virtually any other electronic business-documentation format. It began by providing the digital security and message-receipt validation for Internet communication for MIME (Multipurpose Internet Mail Extensions) packaging of EDI.1 EDI-INT has since become the leading means of business-to-business (B2B) transport for retail and other industries.

Although invisible to the consumer, standards for secure electronic communication of purchase orders, invoices, and other business transactions are helping enterprises drive down costs and offer flexibility in B2B relationships. EDI-INT provides digital security of email, Web, and FTP payloads through authentication, content-integrity, confidentiality, and receipt validation.

ONLINE HANDWRITTEN SCRIPT RECOGNITION

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 paper 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.

Index Terms

Document understanding, handwritten script identification, online document, evidence accumulation, feature design.

LOCATION-AIDED ROUTING (LAR) IN MOBILE AD HOC NETWORKS

A mobile ad hoc network consists of wireless hosts that may move often. Movement of hosts results in a change in routes, requiring some mechanism for determining new routes. Several routing protocols have already been proposed for ad hoc networks.

This paper suggests an approach to utilize location information (for instance, obtained using the global positioning system) to improve performance of routing protocols for ad hoc networks.

By using location information, the proposed Location-Aided Routing (LAR) protocols limit the search for a new route to a smaller “request zone” of the ad hoc network.

This results in a significant reduction in the number of routing messages. We present two algorithms to determine the request zone, and also suggest potential optimizations to our algorithms

NOISE REDUCTION BY FUZZY IMAGE FILTERING

A new fuzzy filter is presented for the noise reduction of images corrupted with additive noise. The filter consists of two stages. The first stage computes a fuzzy derivative for eight different directions.

The second stage uses these fuzzy derivatives to perform fuzzy smoothing by weighting the contributions of neighboring pixel values. Both stages are based on fuzzy rules which make use of membership functions. The filter can be applied iteratively to effectively reduce heavy noise.

In particular, the shape of the membership functions is adapted according to the remaining noise level after each iteration, making use of the distribution of the homogeneity in the image.

A statistical model for the noise distribution can be incorporated to relate the homogeneity to the adaptation scheme of the membership functions. Experimental results are obtained to show the feasibility of the proposed approach.

These results are also compared to other filters by numerical measures and visual inspection.

Index Terms

Additive noise, edge preserving filtering, fuzzy image filtering, noise reduction.

ITP: AN IMAGE TRANSPORT PROTOCOL FOR THE INTERNET

Images account for a significant and growing fraction of Web downloads. The traditional approach to transporting images uses TCP, which provides a generic reliable in-order bytestream abstraction, but which is overly restrictive for image data.

We analyze the progression of image quality at the receiver with time, and show that the in-order delivery abstraction provided by a TCP-based approach prevents the receiver application from processing and rendering portions of an image when they actually arrive.

The end result is that an image is rendered in bursts interspersed with long idle times rather than smoothly. This paper describes the design, implementation, and evaluation of the image transport protocol (ITP) for image transmission over loss-prone congested or wireless networks.

ITP improves user-perceived latency using application-level framing (ALF) and out-of order application data unit (ADU) delivery, achieving significantly better interactive performance as measured by the evolution of peak signal-to-noise ratio (PSNR) with time at the receiver.

ITP runs over UDP, incorporates receiver-driven selective reliability, uses the congestion manager (CM) to adapt to network congestion, and is customizable for specific image formats (e.g., JPEG and JPEG2000). ITP enables a variety of new receiver post-processing algorithms such as error concealment that further improve the interactivity and responsiveness of reconstructed images.

Performance experiments using our implementation across a variety of loss conditions demonstrate the benefits of ITP in improving the interactivity of image downloads at the receiver.

Index Terms

Computer networks, congestion control, Internetworking, network adaptation, selective reliability, transport protocols.

A REPUTATION BASED TRUST MODEL FOR PEER TO PEER ECOMMERCE COMMUNITIES

Peer-to-Peer eCommerce communities are commonly perceived as an environment ordering both opportunities and threats. One way to minimize threats in such an open community is to use community-based reputations, which can be computed, for example, through feedback about peers' transaction histories.

Such reputation information can help estimating the trustworthiness and predicting the future behavior of peers. This paper presents a coherent adaptive trust model for quantifying and comparing the trustworthiness of peers based on a transaction-based feedback system.

There are two main features of our model. First, we argue that the trust models based solely on feedback from other peers in the community is inaccurate and ineffective. We introduce three basic trust parameters in computing trustworthiness of peers.

In addition to feedback a peer receives through its transactions with other peers, we incorporate the total number of transactions a peer performs, and the credibility of the feedback sources into the model for evaluating the trustworthiness of peers.

Second, we introduce two adaptive factors, the transaction context factor and the community context factor, to allow the metric to adapt to different domains and situations and to address common problems encountered in a variety of online communities.

We also developed a concrete method to validate the proposed trust model and obtained initial results, showing the feasibility and benefit of our approach.

EFFICIENT ROUTING IN INTERMITTENTLY CONNECTED MOBILE NETWORKS: THE MULTIPLE-COPY CASE

Intermittently connected mobile networks are wireless networks where most of the time there does not exist a complete path from the source to the destination. There are many real networks that follow this model, for example, wildlife tracking sensor networks, military networks, vehicular ad hoc networks, etc.

In this context, conventional routing schemes fail, because they try to establish complete end-to-end paths, before any data is sent. To deal with such networks researchers have suggested to use flooding-based routing schemes.

While flooding-based schemes have a high probability of delivery, they waste a lot of energy and suffer from severe contention which can significantly degrade their performance. Furthermore, proposed efforts to reduce the overhead of flooding-based schemes have often been plagued by large delays.

With this in mind, we introduce a new family of routing schemes that “spray” a few message copies into the network, and then route each copy independently towards the destination.

We show that, if carefully designed, spray routing not only performs significantly fewer transmissions per message, but also has lower average delivery delays than existing schemes; furthermore, it is highly scalable and retains good performance under a large range of scenarios.

Finally, we use our theoretical framework proposed in our 2004 paper to analyze the performance of spray routing. We also use this theory to show how to choose the number of copies to be sprayed and how to optimally distribute these copies to relays.

Index Terms

Ad hoc networks, delay tolerant networks, intermittent connectivity, routing

MODELING PEER-PEER FILE SHARING SYSTEMS

Peer-peer networking has recently emerged as a new paradigm for building distributed networked applications. In this paper we develop simple mathematical models to explore and illustrate fundamental performance issues of peer-peer file sharing systems. The modeling framework introduced and the corresponding solution method are flexible enough to accommodate different characteristics of such systems.

Through the specification of model parameters, we apply our framework to three different peer-peer architectures: centralized indexing, distributed indexing with flooded queries, and distributed indexing with hashing directed queries.

Using our model, we investigate the effects of system scaling, freeloaders, file popularity and availability on system performance. In particular, we observe that a system with distributed indexing and flooded queries cannot exploit the full capacity of peer-peer systems.

We further show that peer-peer file sharing systems can tolerate a significant number of freeloaders without suffering much performance degradation. In many cases, freeloaders can benefit from the available spare capacity of peer-peer systems and increase overall system throughput.

Our work shows that simple models coupled with efficient solution methods can be used to understand and answer questions related to the performance of peer-peer file sharing systems.

A wireless distributed intrusion detection system and a new attack model Denial-of-Service attacks, and jamming in particular, are a threat to wireless networks because they are at the same time easy to mount and difficult to detect and stop.

We propose a distributed intrusion detection system in which each node monitors the traffic flow on the network and collects relevant statistics about it. By combining each node's view we are able to tell if (and which type of) an attack happened or if the channel is just saturated.

However, this system opens the possibility for misuse. We discuss the impact of the misuse on the system and the best strategies for each actor.

DYNAMIC PARALLEL ACCESS TO REPLICATED CONTENT IN THE INTERNET

Popular content is frequently replicated in multiple servers or caches in the Internet to offload origin servers and improve end-user experience. However, choosing the best server is a nontrivial task and a bad choice may provide poor end user experience.

In contrast to retrieving a file from a single server, we propose a parallel-access scheme where end users access multiple servers at the same time, fetching different portions of that file from different servers and reassembling them locally.

The amount of data retrieved from a particular server depends on the resources available at that server or along the path from the user to the server. Faster servers will deliver bigger portions of a file while slower servers will deliver smaller portions.

If the available resources at a server or along the path change during the download of a file, a dynamic parallel access will automatically shift the load from congested locations to less loaded parts (server and links) of the Internet.

The end result is that users experience significant speedups and very consistent response times. Moreover, there is no need for complicated server selection algorithms and load is dynamically shared among all servers.

The dynamic parallel-access scheme presented in this paper does not require any modifications to servers or content and can be easily included in browsers, peer-to-peer applications or content distribution networks to speed up delivery of popular content.

Index Terms

Content distribution, HTTP, Internet, mirroring, parallel access, peer-to-peer, replication, Web.

A FULLY DISTRIBUTED PROACTIVELY SECURE THRESHOLD-MULTISIGNATURE SCHEME

Threshold-multisignature schemes combine the properties of threshold group-oriented signature schemes and multisignature schemes to yield a signature scheme that allows a threshold 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/updating schemes by giving group members a mechanism to identify malicious or faulty share holders in the first round, thus avoiding multiple protocol executions.

Index Terms

Security and protection, distributed systems, group-oriented cryptography, threshold-multisignature, secret sharing, distributed-key management infrastructure, publicly verifiable distributed-key generation, publicly verifiable distributed-key update, publicly verifiable distributed-key redistribution

A NEW OPERATIONAL TRANSFORMATION FRAMEWORK FOR REAL-TIME GROUP EDITORS

Group editors allow a group of distributed human users to edit a shared multimedia document at the same time over a computer network. Consistency control in this environment must not only guarantee convergence of replicated data, but also attempt to preserve intentions of operations.

Operational transformation (OT) is a well-established method for optimistic consistency control in this context and has drawn continuing research attention since 1989. However, counterexamples to previous works have often been identified despite the significant progress made on this topic over the past 15 years.

This paper analyzes the root of correctness problems in OT and establishes a novel operational transformation framework for developing OT algorithms and proving their correctness.

Index Terms

Consistency control, group editors, groupware, operational transformation

DISTRIBUTED COLLABORATIVE KEY AGREEMENT PROTOCOLS FOR DYNAMIC PEER GROUPS

We consider several distributed collaborative key agreement protocols for dynamic peer groups. This problem has several important characteristics which make it different from traditional secure group communication.

They are

- (1) distributed nature in which there is no centralized key server,**
- (2) collaborative nature in which the group key is contributive; i.e., each group member will collaboratively contribute its part to the global group key, and**
- (3) dynamic nature in which existing members can leave the group while new members may join. Instead of performing individual rekey operations, i.e., recomputing the group key after every join or leave request, we consider an interval based approach of rekeying.**

In particular, we consider three distributed algorithms for updating the group key:

- (1) the Rebuild algorithm,**
- (2) the Batch algorithm, and**
- (3) the Queuebatch algorithm. We analyze the performance of these distributed algorithms under different settings, including different population sizes and different join/leave probabilities.**

We show that these three distributed algorithms significantly outperform the individual rekey algorithm, and that the Queue-batch algorithm performs the best among the three distributed algorithms.

Moreover, the Queue-batch algorithm has the intrinsic property of balancing the computation/ communication workload such that the dynamic peer group can quickly begin secure group communication.

This provides fundamental understanding about establishing a collaborative group key for a distributed dynamic peer group.

TWO TECHNIQUES FOR FAST COMPUTATION OF CONSTRAINED SHORTEST PATHS

Computing constrained shortest paths is fundamental to some important network functions such as QoS routing, MPLS path selection, ATM circuit routing, and traffic engineering. The problem is to find the cheapest path that satisfies certain constraints.

In particular, finding the cheapest delay-constrained path is critical for real-time data flows such as voice/video calls. Because it is NP-complete, much research has been designing heuristic algorithms that solve the approximation of the problem with an adjustable accuracy.

A common approach is to discretize (i.e., scale and round) the link delay or link cost, which transforms the original problem to a simpler one solvable in polynomial time. The efficiency of the algorithms directly relates to the magnitude of the errors introduced during discretization.

In this paper, we propose two techniques that reduce the discretization errors, which allows faster algorithms to be designed. Reducing the overhead of computing constrained shortest paths is practically important for the successful design of a high-throughput QoS router, which is limited at both processing power and memory space.

Our simulations show that the new algorithms reduce the execution time by an order of magnitude on power-law topologies with 1000 nodes. The reduction in memory space is similar.

Index Terms

Approximation algorithms, constrained shortest paths, QoS routing.