Networking for java/ dot net

1. Decentralized Queue Balancing and Differentiated Service Scheme Based on Cooperative Control Concept.

In this paper, we introduce the concept of a bottleneck-routers cooperation in the explicit rate-control framework of communication networks in order to mitigate congestion effects on the network performance and balance the queues. The proposed controller at each router (server or switch) regulates the rates of the heterogeneous source classes leveraging on the cooperation of neighboring bottlenecks. We consider the model of multibottleneck network in the presence of time delay and formulate global stability conditions suitable for network parameters and controller gains design. The proposed approach guarantees good performance in terms of link utilization, packet loss and fairness. Additionally it is guaranteed queue balancing without requiring rerouting or hop-by-hop operation differently from the existing approaches. A validation is carried out by a discrete packet experiment simulator in a realistic multibottleneck scenario to demonstrate the effectiveness of the key idea of the paper. Finally the proposed scheme is compared to some of well-known network controller-type presented in the literature in both steady-state and dynamic network scenario.

2. A Fast Re-Route Method.

Synopsis:

We present a method to find an alternate path, after a link failure, from a source node to a destination node, before the Interior Gateway Protocol (e.g., OSPF or IS-IS) has had a chance to reconverge in response to the failure. The target application is a small (up to tens of nodes) regional access subnetwork of a service provider's network, which is a typical access scale encountered in practice. We illustrate the method and prove that it will find a path if one exists.

3. An Efficient Caching Scheme and Consistency Maintenance in Hybrid P2P System.

Synopsis:

: Peer-to-peer overlay networks are widely used in distributed systems. P2P networks can be divided into two categories: structured peer-to-peer networks in which peers are connected by a regular topology, and unstructured peer-to-peer networks in which the topology is arbitrary. The objective of this work is to design a hybrid peer-to-peer system for distributed data sharing which combines the advantages of both types of peer-to-peer networks and minimizes their disadvantages. Consistency maintenance is propagating the updates from a primary file to its replica. Adaptive consistency maintenance algorithm (ACMA) maintains that periodically polls the file owner to update the file due to minimum number of replicas consistency overhead is very low. Top Caching (TC) algorithm helps to boost the system performance and to build a fully distributed cache for most popular information. Our caching scheme can deliver lower query delay, better load balance and higher cache hit ratios. It effectively relieves the over-caching problems for the most popular objects.

4. A New Multi-path Routing Methodology Based on Logit Type Assignment.

Synopsis:

We present a new multi-path routing methodology called MLB-routing based on multinomial logit model, which is well known as the random utility theory. The key concept of the study is to incorporate multiple paths from same origin to destination, and distribute packets followed by the multinomial logit type probability. Since MLB-routing is pure multi-path routing, it reduce the severe convergence to same links and increases the bandwidth utilization in the network. Compared to the existing multi-path routing schemes that select pre-determined alternate paths, the proposed method can dynamically distribute packets to every possible paths and thus is more efficient than them. Furthermore, it should be mentioned that this methodology could be implemented as both link-state protocol and distance-vector protocol. Therefore, it has enough affinity for present Internet mechanism. Using simulations, we have also shown that this methodology produces more efficient use of network and causes significant improvements in end-to-end delays and jitter times.

5. HALO: Hop-by-Hop Adaptive Link-State Optimal Routing.

Synopsis:

We present HALO, the first link-state routing solution with hop-by-hop packet forwarding that minimizes the cost of carrying traffic through packet-switched networks. At each

node , for every other node , the algorithm independently and iteratively updates

the fraction of traffic destined to that leaves on each of its outgoing links. At each iteration, the updates are calculated based on the shortest path to each destination as determined by the marginal costs of the network's links. The marginal link costs used to find the shortest paths are in turn obtained from link-state updates that are flooded through the network after each iteration. For stationary input traffic, we prove that HALO converges to the routing assignment that minimizes the cost of the network. Furthermore, we observe that our technique is adaptive, automatically converging to the new optimal routing assignment for quasi-static network changes. We also report numerical and experimental evaluations to confirm our theoretical predictions, explore additional aspects of the solution, and outline a proof-of-concept implementation of HALO.

6. Access Policy Consolidation for Event Processing Systems.

Synopsis:

Current event processing systems lack methods to preserve privacy constraints of incoming event streams in a chain of subsequently applied stream operations. This is a problem in large-scale distributed applications like a logistic chain where event processing operators may be spread over multiple security domains. An adversary can infer from legally received outgoing event streams confidential input streams of the event processing system. This paper presents a fine-grained access management for complex event processing. Each incoming event stream can be protected by the specification of an access policy and is enforced by algorithms for access consolidation. The utility of the event processing system is increased by providing and computing in a scalable manner a measure for the obfuscation of event streams. An obfuscation threshold as part of the access policy allows to ignore access requirements and deliver events which have achieved a sufficient high obfuscation level.

7. Auditing for Network Coding Storage.

Synopsis:

Network coding-based storage has recently received a lot of attention in the network coding community. Independently, another body of work has proposed integrity checking schemes for cloud storage, none of which, however, is customized for network coding storage or can efficiently support repair. In this work, we bridge the gap between these currently disconnected bodies of work, and we focus on the (novel) advantage of network coding for integrity checking. We propose NC-Audit - a remote data integrity checking scheme, designed specifically for network coding-based storage cloud. NC-Audit provides a unique combination of desired properties: (i) efficient checking of data integrity (ii) efficient support for repairing failed nodes (iii) full support for modification of outsourced data and (iv) protection against information leakage when checking is performed by a third party. The key ingredient of the design of NC-Audit is a novel combination of SpaceMac, a homomorphic MAC scheme for network coding, and NCrypt, a novel CPA-secure encryption scheme that is compatible with SpaceMac. Our evaluation of a Java implementation of NC-Audit shows that an audit costs the storage node and the auditor only a few milliseconds of computation time, and lower bandwidth than prior work.

8. Buffer Sizing for 802.11 Based Networks.

Synopsis:

We consider the sizing of network buffers in IEEE 802.11-based networks. Wireless networks face a number of fundamental issues that do not arise in wired networks. We demonstrate that the use of fixed-size buffers in 802.11 networks inevitably leads to either undesirable channel underutilization or unnecessary high delays. We present two novel dynamic buffer-sizing algorithms that achieve high throughput while maintaining low delay across a wide range of network conditions. Experimental measurements demonstrate the utility of the proposed algorithms in a production WLAN and a lab test bed.

9. Optimized Multicast Routing Algorithm Based on Tree Structure in MANETs .

Synopsis:

Mobile Ad hoc Networks (MANETs) play an important role in emergency communications where network needs to be constructed temporarily and quickly. Since the nodes move randomly, routing protocols must be highly effective and reliable to guarantee successful packet delivery. Based on the data delivery structure, most of the existing multicast routing protocols can be classified into two folders: tree-based and mesh-based. We observe that tree-based ones have high forwarding efficiency and low consumptions of bandwidth, and they may have poor robustness because only one link exists between two nodes. As a tree-based multicast routing protocol, MAODV (Multicast Ad hoc On-demand Vector) shows an excellent performance in lightweight ad hoc networks. As the load of network increases, QoS (Quality of Service) is degraded obviously. In this paper, we analyze the impact of network load on MAODV protocol, and propose an optimized protocol MAODV-BB (Multicast Ad hoc On-demand Vector with Backup Branches), which improves robustness of the MAODV protocol by combining advantages of the tree structure and the mesh structure. It not only can update shorter tree branches but also construct a multicast tree with backup branches. Mathematical analysis and simulation results both demonstrate that the MAODV-BB protocol improves the network performance over conventional MAODV in heavy load ad hoc networks.

10. Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless Networks.

Synopsis:

The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming. This intentional interference with wireless transmission launch pad for mounting Denial-Of-Service attack on wireless networks. Typically, jamming has been addresses under an external threat model. However, adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this work we address the problem of jamming attacks and adversary is active for short period of time, selectively targeting the messages of high importance. We show that the selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All-Or-Nothing Transformation Hiding Schemes (AONTS-HS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks.

11. FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks.

Synopsis:

Distributed denial-of-service (DDoS) attacks remain a major security problem, the mitigation of which is very hard especially when it comes to highly distributed botnet-based attacks. The early discovery of these attacks, although challenging, is necessary to protect end-users as well as the expensive network infrastructure resources. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of FireCol using extensive simulations and a real dataset is presented, showing FireCol effectiveness and low overhead, as well as its support for incremental deployment in real networks.

12. Delay Analysis and Optimality of Scheduling Policies for Multi-Hop Wireless Networks.

Synopsis:

We analyze the delay performance of a multihop wireless network with a fixed route between each source-destination pair. We develop a new queue grouping technique to handle the complex correlations of the service process resulting from the multihop nature of the flows. A general set-based interference model is assumed that imposes constraints on links that can be served simultaneously at any given time. These interference constraints are used to obtain a fundamental lower bound on the delay performance of any scheduling policy for the system. We present a systematic methodology to derive such lower bounds. For a special wireless system, namely the clique, we design a policy that is sample-path delay-optimal. For the tandem queue network, where the delay-optimal policy is known, the expected delay of the optimal policy numerically coincides with the lower bound. We conduct extensive numerical studies to suggest that the average delay of the back-pressure scheduling policy can be made close to the lower bound by using appropriate functions of queue length.

13. Scaling Laws for Throughput Capacity and Delay in Wireless Networks – A Survey.

Synopsis:

The capacity scaling law of wireless networks has been considered as one of the most fundamental issues. In this survey, we aim at providing a comprehensive overview of the development in the area of scaling laws for throughput capacity and delay in wireless networks. We begin with background information on the notion of throughput capacity of random networks. Based on the benchmark random network model, we then elaborate the advanced strategies adopted to improve the throughput capacity, and other factors that affect the scaling laws. We also present the fundamental tradeoffs between throughput capacity and delay under a variety of mobility models. In addition, the capacity and delay for hybrid wireless networks are surveyed, in which there are at least two types of nodes functioning differently, e.g., normal nodes and infrastructure nodes. Finally, recent studies on scaling law for throughput capacity and delay in emerging vehicular networks are introduced.

14. Cross-Domain Privacy-Preserving Cooperative Firewall Optimization.

Synopsis:

Firewalls have been widely deployed on the Internet for securing private networks. A firewall checks each incoming or outgoing packet to decide whether to accept or discard the packet based on its policy. Optimizing firewall policies is crucial for improving network performance. Prior work on firewall optimization focuses on either intra-firewall or inter-firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. This paper explores inter-firewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. In this paper, we propose the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other. We implemented our protocol and conducted extensive experiments. The results on real firewall policies show that our protocol can remove as many as 49% of the rules in a firewall whereas the average is 19.4%. The communication cost is less than a few hundred KBs. Our protocol incurs no extra online packet processing overhead and the offline processing time is less than a few hundred seconds.

15. Game-Theoretic Pricing for Video Streaming in Mobile Networks.

Synopsis:

Mobile phones are among the most popular consumer devices, and the recent developments of 3G networks and smart phones enable users to watch video programs by subscribing data plans from service providers. Due to the ubiquity of mobile phones and phone-to-phone communication technologies, data-plan subscribers can redistribute the video content to nonsubscribers. Such a redistribution mechanism is a potential competitor for the mobile service provider and is very difficult to trace given users' high mobility. The service provider has to set a reasonable price for the data plan to prevent such unauthorized redistribution behavior to protect or maximize his/her own profit. In this paper, we analyze the optimal price setting for the service provider by investigating the equilibrium between the subscribers and the secondary buyers in the content-redistribution network. We model the behavior between the subscribers and the secondary buyers as a noncooperative game and find the optimal price and quantity for both groups of users. Based on the behavior of users in the redistribution network, we investigate the evolutionarily stable ratio of mobile users who decide to subscribe to the data plan. Such an analysis can help the service provider preserve his/her profit under the threat of the redistribution networks and can improve the quality of service for end users.

16. Locating Equivalent Servants over P2P Networks.

Synopsis:

While peer-to-peer networks are mainly used to locate unique resources across the Internet, new interesting deployment scenarios are emerging. Particularly, some applications (e.g., VoIP) are proposing the creation of overlays for the localization of services based on equivalent servants (e.g., voice relays). This paper explores the possible overlay architectures that can be adopted to provide such services, showing how an unstructured solution based on a scale-free overlay topology is an effective option to deploy in this context. Consequently, we propose EQUATOR (EQUivalent servAnt locaTOR), an unstructured overlay implementing the above mentioned operating principles, based on an overlay construction algorithm that well approximates an ideal scale-free construction model. We present both analytical and simulation results which support our overlay topology selection and validate the proposed architecture.

17. Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks.

Synopsis:

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

18. Fault Node Recovery Algorithm for a Wireless Sensor Network.

Synopsis:

This paper proposes a fault node recovery algorithm to enhance the lifetime of a wireless sensor network when some of the sensor nodes shut down. The algorithm is based on the grade diffusion algorithm combined with the genetic algorithm. The algorithm can result in fewer replacements of sensor nodes and more reused routing paths. In our simulation, the proposed algorithm increases the number of active nodes up to 8.7 times, reduces the rate of data loss by approximately 98.8%, and reduces the rate of energy consumption by approximately 31.1%.

19. Handling Multiple Failures in IP Networks through Localized On-Demand Link State Routing.

Synopsis:

It has been observed that transient failures are fairly common in IP backbone networks and there have been several proposals based on local rerouting to provide high network availability despite failures. While most of these proposals are effective in handling single failures, they either cause loops or drop packets in the case of multiple independent failures. To ensure forwarding continuity even with multiple failures, we propose Localized On-demand Link State (LOLS) routing. Under LOLS, each packet carries a blacklist, which is a minimal set of failed links encountered along its path, and the next hop is determined by excluding the blacklisted links. We show that the blacklist can be reset when the packet makes forward progress towards the destination and hence can be encoded in a few bits. Furthermore, blacklist-based forwarding entries at a router can be precomputed for a given set of failures requiring protection. While the LOLS approach is generic, this paper describes how it can be applied to ensure forwarding to all reachable destinations in case of any two link or node failures. Our evaluation of this failure scenario based on various real network topologies reveals that LOLS needs 6 bits in the worst case to convey the blacklist information. We argue that this overhead is acceptable considering that LOLS routing deviates from the optimal path by a small stretch only while routing around failures.

20. ProgME: Towards Programmable Network Measurement.

Synopsis:

Traffic measurements provide critical input for a wide range of network management applications, including traffic engineering, accounting, and security analysis. Existing measurement tools collect traffic statistics based on some predetermined, inflexible concept of “flows.” They do not have sufficient built-in intelligence to understand the application requirements or adapt to the traffic conditions. Consequently, they have limited scalability with respect to the number of flows and the heterogeneity of monitoring applications. We present ProgME, a Programmable MEasurement architecture based on a novel concept of flowset-an arbitrary set of flows defined according to application requirements and/or traffic conditions. Through a simple flowset composition language, ProgME can incorporate application requirements, adapt itself to circumvent the scalability challenges posed by the large number of flows, and achieve a better application-perceived accuracy. The modular design of ProgME enables it to exploit the surging popularity of multicore processors to cope with 7-Gb/s line rate. ProgME can analyze and adapt to traffic statistics in real time. Using sequential hypothesis test, ProgME can achieve fast and scalable heavy hitter identification

21. Fully Anonymous Profile Matching in Mobile Social Networks.

Synopsis:

In this paper, we study user profile matching with privacy-preservation in mobile social networks (MSNs) and introduce a family of novel profile matching protocols. We first propose an explicit Comparison-based Profile Matching protocol (eCPM) which runs between two parties, an initiator and a responder. The eCPM enables the initiator to obtain the comparison-based matching result about a specified attribute in their profiles, while preventing their attribute values from disclosure. We then propose an implicit Comparison-based Profile Matching protocol (iCPM) which allows the initiator to directly obtain some messages instead of the comparison result from the responder. The messages unrelated to user profile can be divided into multiple categories by the responder. The initiator implicitly chooses the interested category which is unknown to the responder. Two messages in each category are prepared by the responder, and only one message can be obtained by the initiator according to the comparison result on a single attribute. We further generalize the iCPM to an implicit Predicate-based Profile Matching protocol (iPPM) which allows complex comparison criteria spanning multiple attributes. The anonymity analysis shows all these protocols achieve the confidentiality of user profiles. In addition, the eCPM reveals the comparison result to the initiator and provides only conditional anonymity; the iCPM and the iPPM do not reveal the result at all and provide full anonymity. We analyze the communication overhead and the anonymity strength of the protocols. We then present an enhanced version of the eCPM, called eCPM+, by combining the eCPM with a novel prediction-based adaptive pseudonym change strategy. The performance of the eCPM and the eCPM+ are comparatively studied through extensive trace-based simulations. Simulation results demonstrate that the eCPM+ achieves significantly higher anonymity strength with slightly larger number of pseudonyms than the eCPM.

22. Independent Directed Acyclic Graphs for Resilient Multipath Routing.

Synopsis:

In order to achieve resilient multipath routing, we introduce the concept of independent directed acyclic graphs (IDAGs) in this paper. Link-independent (node-independent) DAGs satisfy the property that any path from a source to the root on one DAG is link-disjoint (node-disjoint) with any path from the source to the root on the other DAG. Given a network, we develop polynomial-time algorithms to compute link-independent and node-independent DAGs. The algorithm developed in this paper: 1) provides multipath routing; 2) utilizes all possible edges; 3) guarantees recovery from single link failure; and 4) achieves all these with at most one bit per packet as overhead when routing is based on destination address and incoming edge. We show the effectiveness of the proposed IDAGs approach by comparing key performance indices to that of the independent trees and multiple pairs of independent trees techniques through extensive simulations.

23. Selfish Overlay Network Creation and Maintenance.

Synopsis:

A foundational issue underlying many overlay network applications ranging from routing to peer-to-peer file sharing is that of the network formation, i.e., folding new arrivals into an existing overlay, and rewiring to cope with changing network conditions. Previous work has considered the problem from two perspectives: devising practical heuristics for the case of cooperative peers and performing game-theoretic analysis for the case of selfish peers. In this paper, we unify the aforementioned thrusts by defining and studying the selfish neighbor selection (SNS) game and its application to overlay routing. At the heart of SNS stands the restriction that peers are allowed up to a certain number of neighbors. This makes SNS substantially different from existing network formation games that impose no bounds on peer degrees. Having bounded degrees has important practical consequences as it permits the creation of overlay structures that require $O(n)$ instead of $O(n^2)$ link monitoring overhead. We show that a node's “best response” wiring strategy amounts to solving a *k* -median problem on asymmetric distance. Best-response wirings have substantial practical utility as they permit selfish nodes to reap substantial performance benefits when connecting to overlays of nonselfish nodes. A more intricate consequence is that even nonselfish nodes can benefit from the existence of some selfish nodes since the latter, via their local optimizations, create a highly optimized backbone, upon which even simple heuristic wirings yield good performance. To capitalize on the above properties, we design, build, and deploy EGOIST, an SNS-inspired prototype overlay routing system for PlanetLab. We demonstrate that EGOIST outperforms existing heuristic overlays on a variety of performance metrics, including delay, available bandwidth, and node utilization, while it remains competitive with an optimal but unscalable full-mesh over- ay.

24. On the Role of Mobility for Multi-message Gossip.

Synopsis:

We consider information dissemination in a large *n* -user wireless network in which *k* users wish to share a unique message with all other users. Each of the *n* users only has knowledge of its own contents and state information; this corresponds to a one-sided push-only scenario. The goal is to disseminate all messages efficiently, hopefully achieving an order-optimal spreading rate over unicast wireless random networks. First, we show that a random-push strategy-where a user sends its own or a received packet at random-is order-wise suboptimal in a random geometric graph: specifically, $\Omega(\sqrt{n})$ times slower than optimal spreading. It is known that this gap can be closed if each user has “full” mobility, since this effectively creates a complete graph. We instead consider velocity-constrained mobility where at each time slot the user moves locally using a discrete random walk with velocity $v(n)$ that is much lower than full mobility. We propose a simple two-stage dissemination strategy that alternates between individual message flooding (“self promotion”) and random gossiping. We prove that this scheme achieves a close to optimal spreading rate (within only a logarithmic gap) as long as the velocity is at least $v(n)=\omega(\sqrt{(\log n/k)})$. The key insight is that the mixing property introduced by the partial mobility helps users to spread in space within a relatively short period compared to the optimal spreading time, which macroscopically mimics message dissemination over a complete graph.

25. MeasuRouting: A Framework for Routing Assisted Traffic Monitoring.

Synopsis:

Monitoring transit traffic at one or more points in a network is of interest to network operators for reasons of traffic accounting, debugging or troubleshooting, forensics, and traffic engineering. Previous research in the area has focused on deriving a placement of monitors across the network toward the end of maximizing the monitoring utility of the network operator for a given traffic routing. However, both traffic characteristics and measurement objectives can dynamically change over time, rendering a previously optimal placement of monitors suboptimal. It is not feasible to dynamically redeploy/reconfigure measurement infrastructure to cater to such evolving measurement requirements. We address this problem by strategically routing traffic subpopulations over fixed monitors. We refer to this approach as MeasuRouting. The main challenge for MeasuRouting is to work within the constraints of existing intradomain traffic engineering operations that are geared for efficiently utilizing bandwidth resources, or meeting quality-of-service (QoS) constraints, or both. A fundamental feature of intradomain routing, which makes MeasuRouting feasible, is that intradomain routing is often specified for aggregate flows. MeasuRouting can therefore differentially route components of an aggregate flow while ensuring that the aggregate placement is compliant to original traffic engineering objectives. In this paper, we present a theoretical framework for MeasuRouting. Furthermore, as proofs of concept, we present synthetic and practical monitoring applications to showcase the utility enhancement achieved with MeasuRouting.

26. SPAF: Stateless FSA-based Packet Filters.

Synopsis:

We propose a stateless packet filtering technique based on finite-state automata (FSA). FSAs provide a comprehensive framework with well-defined composition operations that enable the generation of stateless filters from high-level specifications and their compilation into efficient executable code without resorting to various opportunistic optimization algorithms. In contrast with most traditional approaches, memory safety and termination can be enforced with minimal run-time overhead even in cyclic filters, thus enabling full parsing of complex protocols and supporting recursive encapsulation relationships. Experimental evidence shows that this approach is viable and improves the state of the art in terms of filter flexibility, performance, and scalability without incurring in the most common FSA deficiencies, such as state-space explosion.

27. Optimizing Cloud Resources for Delivering IPTV Services through Virtualization.

Synopsis:

Virtualized cloud-based services can take advantage of statistical multiplexing across applications to yield significant cost savings. However, achieving similar savings with real-time services can be a challenge. In this paper, we seek to lower a provider's costs for real-time IPTV services through a virtualized IPTV architecture and through intelligent time-shifting of selected services. Using Live TV and Video-on-Demand (VoD) as examples, we show that we can take advantage of the different deadlines associated with each service to effectively multiplex these services. We provide a generalized framework for computing the amount of resources needed to support multiple services, without missing the deadline for any service. We construct the problem as an optimization formulation that uses a generic cost function. We consider multiple forms for the cost function (e.g., maximum, convex and concave functions) reflecting the cost of providing the service. The solution to this formulation gives the number of servers needed at different time instants to support these services. We implement a simple mechanism for time-shifting scheduled jobs in a simulator and study the reduction in server load using real traces from an operational IPTV network.

Our results show that we are able to reduce the load by ~24%(compared to a possible ~31.3% as predicted by the optimization framework).

28. Packet Loss Control Using Tokens at the Network Edge.

Synopsis:

Presently, the Internet accommodates simultaneous audio, video, and data traffic. This requires the Internet to guarantee the packet loss which at its turn depends very much on congestion control. A series of protocols have been introduced to supplement the insufficient TCP mechanism controlling the network congestion. CSFQ was designed as an open-loop controller to provide the fair best effort service for supervising the per-flow bandwidth consumption and has become helpless when the P2P flows started to dominate the traffic of the Internet. Token-Based Congestion Control (TBCC) is based on a closed-loop congestion control principle, which restricts token resources consumed by an end-user and provides the fair best effort service with O(1) complexity. As Self-Verifying CSFQ and Re-feedback, it experiences a heavy load by policing inter-domain traffic for lack of trust. In this paper, Stable Token-Limited Congestion Control (STLCC) is introduced as new protocols which appends inter-domain congestion control to TBCC and make the congestion control system to be stable. STLCC is able to shape output and input traffic at the inter-domain link with O(1) complexity. STLCC produces a congestion index, pushes the packet loss to the network edge and improves the network performance. Finally, the simple version of STLCC is introduced. This version is deployable in the Internet without any IP protocols modifications and preserves also the packet datagram.

29. TrickleDNS: Bootstrapping DNS Security using Social Trust.

Synopsis:

This paper presents TrickleDNS, a decentralized system for proactive dissemination of DNS data. Unlike prior solutions, which depend on the complete deployment of DNSSEC standard to preserve data integrity, TrickleDNS offers an incrementally deployable solution with a probabilistic guarantee on data integrity that becomes stronger as the adoption of DNSSEC increases. TrickleDNS provides resilience from data corruption attacks and denial of service attacks, including sybil attacks, using three key steps. First, TrickleDNS organizes participating nameservers into a well-connected peer-to-peer Secure Network of Nameservers (SNN) using two types of trust links: (a) strongly trusted social relationships across DNS servers (which exist today); (b) random yet constrained weak trust links between DNS servers, which it introduces. The SNN allows nameservers in the network to reliably broadcast their public-keys to each other without relying on a centralized PKI.

Second, TrickleDNS reliably binds domains to their authoritative name servers through independent verification by multiple, randomly chosen peers within the SNN. Finally, TrickleDNS servers proactively disseminate self-certified versions of DNS records to provide faster performance, better availability, and improved security.

30. Policy-by-Example for Online Social Networks.

Synopsis:

We introduce two approaches for improving privacy policy management in online social networks. First, we introduce a mechanism using proven clustering techniques that assists users in grouping their friends for group based policy management approaches. Second, we introduce a policy management approach that leverages a user's memory and opinion of their friends to set policies for other similar friends. We refer to this new approach as Same-As Policy Management. To demonstrate the effectiveness of our policy management improvements, we implemented a prototype Facebook application and conducted an extensive user study. Leveraging proven clustering techniques, we demonstrated a 23% reduction in friend grouping time. In addition, we demonstrated considerable reductions in policy authoring time using Same-As Policy Management over traditional group based policy management approaches. Finally, we presented user perceptions of both improvements, which are very encouraging.

31. Optimum Relay Selection for Energy-Efficient Cooperative Ad Hoc Networks.

Synopsis:

The Cooperative Communication (CC) is a technology that allows multiple nodes to simultaneously transmit the same data. It can save power and extend transmission coverage. However, prior research work on topology control considers CC only in the aspect of energy saving, not that of coverage extension. We identify the challenges in the development of a centralized topology control scheme, named Cooperative Bridges, which reduces transmission power of nodes as well as increases network connectivity. Prior research on topology control with CC only focuses on maintaining the network connectivity, minimizing the transmission power of each node, whereas ignores the energy efficiency of paths in constructed topologies. This may cause inefficient routes and hurt the overall network performance in cooperative ad hoc networks. In this paper, to address this problem, we studied topology control problem for energy-efficient topology control problem with cooperative communication. We proposed optimum relay nodes selection for CC network to reduce overall power consumption of network

32. Participatory Privacy: Enabling Privacy in Participatory Sensing.

Synopsis:

Participatory sensing is an emerging computing paradigm that enables the distributed collection of data by self-selected participants. It allows the increasing number of mobile phone users to share local knowledge acquired by their sensor-equipped devices (e.g., to monitor temperature, pollution level, or consumer pricing information). While research initiatives and prototypes proliferate, their real-world impact is often bounded to comprehensive user participation. If users have no incentive, or feel that their privacy might be endangered, it is likely that they will not participate. In this article, we focus on privacy protection in participatory sensing and introduce a suitable privacy-enhanced infrastructure. First, we provide a set of definitions of privacy requirements for both data producers (i.e., users providing sensed information) and consumers (i.e., applications accessing the data). Then we propose an efficient solution designed for mobile phone users, which incurs very low overhead. Finally, we discuss a number of open problems and possible research directions.

33. Price Differentiation for Communication Networks

Synopsis:

We study the optimal usage-based pricing problem in a resource-constrained network with one profit-maximizing service provider and multiple groups of surplus-maximizing users. With the assumption that the service provider knows the utility function of each user (thus complete information), we find that the complete price differentiation scheme can achieve a large revenue gain (e.g., 50%) compared to no price differentiation, when the total network resource is comparably limited and the high-willingness-to-pay users are minorities. However, the complete price differentiation scheme may lead to a high implementational complexity. To trade off the revenue against the implementational complexity, we further study the partial price differentiation scheme and design a polynomial-time algorithm that can compute the optimal partial differentiation prices. We also consider the incomplete information case where the service provider does not know to which group each user belongs. We show that it is still possible to realize price differentiation under this scenario and provide the sufficient and necessary condition under which an incentive-compatible differentiation scheme can achieve the same revenue as under complete information.

34. Reliable Data Delivery in Mobile Adhoc Networks Using Light Weight Verification Algorithm with High Node Mobility .

Synopsis:

This paper addresses data aggregation and data packets issues for highly dynamic mobile ad hoc networks and Wireless Sensor Networks thereby leading to a timely and reliable reduction in both communication and energy consumption. But there might be node failures in existing systems and an aggregation framework does not address issues of false subaggregate values due to compromised nodes leading to huge errors in base station computed aggregates when data is transferred through mobile sensor nodes. It cannot also transfer data after nodes fail at the intermediate level. This paper proposes a novel lightweight verification algorithm and Position-based Opportunistic Routing (POR) protocol which reduces node failure and data loss issues. Theoretical analysis and simulation prove that POR and the novel lightweight verification algorithm achieve excellent performance under high node mobility with acceptable overhead. Also the new void handling scheme performs efficiently.

35. Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing

Synopsis:

In cloud computing, data generated in electronic form are large in amount. To maintain this data efficiently, there is a necessity of data recovery services. To cater this, in this paper we propose a smart remote data backup algorithm, Seed Block Algorithm (SBA). The objective of proposed algorithm is twofold, first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any reason. The time related issues are also being solved by proposed SBA such that it will take minimum time for the recovery process. Proposed SBA also focuses on the security concept for the back-up files stored at remote server, without using any of the existing encryption techniques.

36. Topological Conditions for In-Network Stabilization of Dynamical Systems.

Synopsis:

We study the problem of stabilizing a linear system over a wireless network using a simple in-network computation method. Specifically, we study an architecture called the "Wireless Control Network" (WCN), where each wireless node maintains a state, and periodically updates it as a linear combination of neighboring plant outputs and node states. This architecture has previously been shown to have low computational overhead and beneficial scheduling and compositionality properties. In this paper we characterize fundamental topological conditions to allow stabilization using such a scheme. To achieve this, we exploit the fact that the WCN scheme causes the network to act as a linear dynamical system, and analyze the coupling between the plant's dynamics and the dynamics of the network. We show that stabilizing control inputs can be computed in-network if the vertex connectivity of the network is larger than the geometric multiplicity of any unstable eigenvalue of the plant. This condition is analogous to the typical min-cut condition required in classical information dissemination problems. Furthermore, we specify equivalent topological conditions for stabilization over a wired (or point-to-point) network that employs network coding in a traditional way - as a communication mechanism between the plant's sensors and decentralized controllers at the actuators.

37. Using Fuzzy Logic Control to Provide Intelligent Traffic Management Service for High-Speed Networks

Synopsis:

In view of the fast-growing Internet traffic, this paper propose a distributed traffic management framework, in which routers are deployed with intelligent data rate controllers to tackle the traffic mass. Unlike other explicit traffic control protocols that have to estimate network parameters (e.g., link latency, bottleneck bandwidth, packet loss rate, or the number of flows) in order to compute the allowed source sending rate, our fuzzy-logic-based controller can measure the router queue size directly; hence it avoids various potential performance problems arising from parameter estimations while reducing much consumption of computation and memory resources in routers. As a network parameter, the queue size can be accurately monitored and used to proactively decide if action should be taken to regulate the source sending rate, thus increasing the resilience of the network to traffic congestion. The communication QoS (Quality of Service) is assured by the good performances of our scheme such as max-min fairness, low queueing delay and good robustness to network dynamics. Simulation results and comparisons have verified the effectiveness and showed that our new traffic management scheme can achieve better performances than the existing protocols that rely on the estimation of network parameters.

38. Cooperation Versus Multiplexing: Multicast Scheduling Algorithms for OFDMA Relay Networks.

Synopsis:

With the next-generation cellular networks making a transition toward smaller cells, two-hop orthogonal frequency-division multiple access (OFDMA) relay networks have become a dominant, mandatory component in the 4G standards (WiMAX 802.16j, 3GPP LTE-Adv). While unicast flows have received reasonable attention in two-hop OFDMA relay networks, not much light has been shed on the design of efficient scheduling algorithms for multicast flows. Given the growing importance of multimedia broadcast and multicast services (MBMS) in 4G networks, the latter forms the focus of this paper. We show that while relay cooperation is critical for improving multicast performance, it must be carefully balanced with the ability to multiplex multicast sessions and hence maximize aggregate multicast flow. To this end, we highlight strategies that carefully group relays for cooperation to achieve this balance. We then solve the multicast scheduling problem under two OFDMA subchannelization models. We establish the NP-hardness of the scheduling problem even for the simpler model and provide efficient algorithms with approximation guarantees under both models. Evaluation of the proposed solutions reveals the efficiency of the scheduling algorithms as well as the significant benefits obtained from the multicasting strategy.

39. A Rank Correlation Based Detection against Distributed Reflection DoS Attacks.

Synopsis:

DDoS presents a serious threat to the Internet since its inception, where lots of controlled hosts flood the victim site with massive packets. Moreover, in Distributed Reflection DoS (DRDoS), attackers fool innocent servers (reflectors) into flushing packets to the victim. But most of current DRDoS detection mechanisms are associated with specific protocols and cannot be used for unknown protocols. It is found that because of being stimulated by the same attacking flow, the responsive flows from reflectors have inherent relations: the packet rate of one converged responsive flow may have linear relationships with another. Based on this observation, the Rank Correlation based Detection (RCD) algorithm is proposed. The preliminary simulations indicate that RCD can differentiate reflection flows from legitimate ones efficiently and effectively, thus can be used as a useable indicator for DRDoS.

40. A Keyless Approach to Image Encryption

Synopsis:

Maintaining the secrecy and confidentiality of images is a vibrant area of research, with two different approaches being followed, the first being encrypting the images through encryption algorithms using keys, the other approach involves dividing the image into random shares to maintain the images secrecy. Unfortunately heavy computation cost and key management limit the employment of the first approach and the poor quality of the recovered image from the random shares limit the applications of the second approach. In this paper we propose a novel approach without the use of encryption keys. The approach employs Sieving, Division and Shuffling to generate random shares such that with minimal computation, the original secret image can be recovered from the random shares without any loss of image quality.

41. Retransmission Delays With Bounded Packets: Power-Law Body and Exponential Tail.

Synopsis:

Retransmissions serve as the basic building block that communication protocols use to achieve reliable data transfer. Until recently, the number of retransmissions was thought to follow a geometric (light-tailed) distribution. However, recent work shows that when the distribution of the packet sizes have infinite support, retransmission-based protocols may result in heavy-tailed delays and possibly zero throughput even when the aforementioned distribution is light-tailed. In reality, however, packet sizes are often bounded by the maximum transmission unit (MTU), and thus the aforementioned result merits a deeper investigation. To that end, in this paper, we allow the distribution of the packet size L to have finite support. Under mild conditions, we show that the transmission duration distribution exhibits a transition from a power-law main body to an exponential tail. The timescale to observe the power-law main body is roughly equal to the average transmission duration of the longest packet. The power-law main body, if significant, may cause the channel throughput to be very close to zero. These theoretical findings provide an understanding on why some empirical measurements suggest heavy tails. We use these results to further highlight the engineering implications of distributions with power-law main bodies and light tails by analyzing two cases: 1) the throughput of on-off channels with retransmissions, where we show that even when packet sizes have small means and bounded support the variability in their sizes can greatly impact system performance; 2) the distribution of the number of jobs in an M/M/∞ queue with server failures. Here, we show that retransmissions can cause long-range dependence and quantify the impact of the maximum job sizes on the long-range dependence.

42. D2P: Distributed Dynamic Pricing Policyin Smart Grid for PHEVs Management.

Synopsis:

Future large-scale deployment of plug-in hybrid electric vehicles (PHEVs) will render massive energy demand on the electric grid during peak-hours. We propose an intelligent distributed dynamic pricing (D2P) mechanism for the charging of PHEVs in a smart grid architecture-an effort towards optimizing the energy consumption profile of PHEVs users. Each micro-grid decides realtime dynamic price as home-price and roaming-price, depending on the supply-demand curve, to optimize its revenue. Consequently, two types of energy services are considered-home micro-grid energy, and foreign micro-grid energy. After designing the PHEVs' mobility and battery models, the pricing policies for the home-price and the roaming-price are presented. A decision making process to implement a cost-effective charging and discharging method for PHEVs is also demonstrated based on the real-time price decided by the micro-grids. We evaluate and compare the results of distributed pricing policy with other existing centralized/distributed ones. Simulation results show that using the proposed architecture, the utility corresponding to the PHEVs increases by approximately 34 percent over that of the existing ones for optimal charging of PHEVs.

43. A New Cell-Counting-Based Attack Against Tor .

Synopsis:

Various low-latency anonymous communication systems such as Tor and Anonymizer have been designed to provide anonymity service for users. In order to hide the communication of users, most of the anonymity systems pack the application data into equal-sized cells (e.g., 512 B for Tor, a known real-world, circuit-based, low-latency anonymous communication network). Via extensive experiments on Tor, we found that the size of IP packets in the Tor network can be very dynamic because a cell is an application concept and the IP layer may repack cells. Based on this finding, we investigate a new cell-counting-based attack against Tor, which allows the attacker to confirm anonymous communication relationship among users very quickly. In this attack, by marginally varying the number of cells in the target traffic at the malicious exit onion router, the attacker can embed a secret signal into the variation of cell counter of the target traffic. The embedded signal will be carried along with the target traffic and arrive at the malicious entry onion router. Then, an accomplice of the attacker at the malicious entry onion router will detect the embedded signal based on the received cells and confirm the communication relationship among users. We have implemented this attack against Tor, and our experimental data validate its feasibility and effectiveness. There are several unique features of this attack. First, this attack is highly efficient and can confirm very short communication sessions with only tens of cells. Second, this attack is effective, and its detection rate approaches 100% with a very low false positive rate. Third, it is possible to implement the attack in a way that appears to be very difficult for honest participants to detect (e.g., using our hopping-based signal embedding).

44. Exploiting Cooperative Relay for High Performance Communications in MIMO Ad Hoc Networks.

Synopsis:

With the popularity of wireless devices and the increase of computing and storage resources, there are increasing interests in supporting mobile computing techniques. Particularly, ad hoc networks can potentially connect different wireless devices to enable more powerful wireless applications and mobile computing capabilities. To meet the ever increasing communication need, it is important to improve the network throughput while guaranteeing transmission reliability. Multiple-input-multiple-output (MIMO) technology can provide significantly higher data rate in ad hoc networks where nodes are equipped with multiantenna arrays. Although MIMO technique itself can support diversity transmission when channel condition degrades, the use of diversity transmission often compromises the multiplexing gain and is also not enough to deal with extremely weak channel. Instead, in this work, we exploit the use of cooperative relay transmission (which is often used in a single antenna environment to improve reliability) in a MIMO-based ad hoc network to cope with harsh channel condition. We design both centralized and distributed scheduling algorithms to support adaptive use of cooperative relay transmission when the direct transmission cannot be successfully performed. Our algorithm effectively exploits the cooperative multiplexing gain and cooperative diversity gain to achieve higher data rate and higher reliability under various channel conditions. Our scheduling scheme can efficiently invoke relay transmission without introducing significant signaling overhead as conventional relay schemes, and seamlessly integrate relay transmission with multiplexed MIMO transmission. We also design a MAC protocol to implement the distributed algorithm. Our performance results demonstrate that the use of cooperative relay in a MIMO framework could bring in a significant throughput improvement in all the scenarios studied, with the variation of node density, link failure ratio, packet arrival - ate, and retransmission threshold.

45. On the Payoff Mechanisms in Peer-Assisted Services With Multiple Content Providers: Rationality and Fairness.

Synopsis:

This paper studies an incentive structure for cooperation and its stability in peer-assisted services when there exist multiple content providers, using a coalition game-theoretic approach. We first consider a generalized coalition structure consisting of multiple providers with many assisting peers, where peers assist providers to reduce the operational cost in content distribution. To distribute the profit from cost reduction to players (i.e, providers and peers), we then establish a generalized formula for individual payoffs when a “Shapley-like” payoff mechanism is adopted. We show that the grand coalition is unstable, even when the operational cost functions are concave, which is in sharp contrast to the recently studied case of a single provider where the grand coalition is stable. We also show that irrespective of stability of the grand coalition, there always exist coalition structures that are not convergent to the grand coalition under a dynamic among coalition structures. Our results give us an incontestable fact that a provider does not tend to cooperate with other providers in peer-assisted services and is separated from them. Three facets of the noncooperative (selfish) providers are illustrated: 1) underpaid peers; 2) service monopoly; and 3) oscillatory coalition structure. Lastly, we propose a stable payoff mechanism that improves fairness of profit sharing by regulating the selfishness of the players as well as grants the content providers a limited right of realistic bargaining. Our study opens many new questions such as realistic and efficient incentive structures and the tradeoffs between fairness and individual providers' competition in peer-assisted services.

46. Designing Truthful Spectrum Double Auctions with Local Markets.

Synopsis:

Market-driven spectrum auctions offer an efficient way to improve spectrum utilization by transferring unused or underused spectrum from its primary license holder to spectrum-deficient secondary users. Such a spectrum market exhibits strong locality in two aspects: 1) that spectrum is a local resource and can only be traded to users within the license area, and 2) that holders can partition the entire license areas and sell any pieces in the market. We design a spectrum double auction that incorporates such locality in spectrum markets, while keeping the auction economically robust and computationally efficient. Our designs are tailored to cases with and without the knowledge of bid distributions. Complementary simulation studies show that spectrum utilization can be significantly improved when distribution information is available. Therefore, an auctioneer can start from one design without any a priori information, and then switch to the other alternative after accumulating sufficient distribution knowledge. With minor modifications, our designs are also effective for a profit-driven auctioneer aiming to maximize the auction revenue.

47. Target Tracking and Mobile Sensor Navigation in Wireless Sensor Networks

Synopsis:

This work studies the problem of tracking signal-emitting mobile targets using navigated mobile sensors based on signal reception. Since the mobile target's maneuver is unknown, the mobile sensor controller utilizes the measurement collected by a wireless sensor network in terms of the mobile target signal's time of arrival (TOA). The mobile sensor controller acquires the TOA measurement information from both the mobile target and the mobile sensor for estimating their locations before directing the mobile sensor's movement to follow the target. We propose a min-max approximation approach to estimate the location for tracking which can be efficiently solved via semidefinite programming (SDP) relaxation, and apply a cubic function for mobile sensor navigation. We estimate the location of the mobile sensor and target jointly to improve the tracking accuracy. To further improve the system performance, we propose a weighted tracking algorithm by using the measurement information more efficiently. Our results demonstrate that the proposed algorithm provides good tracking performance and can quickly direct the mobile sensor to follow the mobile target.

48. A Reliable Multi Grid Routing Protocol for Tactical MANET..

Synopsis:

We propose a reliable multi-grid based routing protocol with the purpose of attaining high percentage of data delivery in the tactical mobile ad hoc networks. In grid-based protocols, deployment region is divided into small patches called ‘cells,’ which are the units of routing. Our routing protocol for tactical MANETs employs multi-grid routing scheme adaptively uses varying cell sizes, unlike single-grid based protocols. In a dense network, a small-cell grid is employed to serve more alternative cells for a path. Meanwhile, a large-cell can be used to allow the probability of seamless data forwarding when the network is sparse. Moreover, we propose two reliability metrics for the grid-based protocol based on packet delivery rate between the cells and the status of the mobile nodes that enables relay node selection in the cell for forwarding data. The results from the performance evaluation in network simulator (ns-2.33) shows that our scheme shows high reliability over 90% of data delivery ratio, low-latency and better overhead compared to the existing routing protocols.

49. Performance analysis of OSPF and EIGRP routing protocols for greener internetworking.

Synopsis:

Routing protocol is taking a vital role in the modern internet era. A routing protocol determines how the routers communicate with each other to forward the packets by taking the optimal path to travel from a source node to a destination node. In this paper we have explored two eminent protocols namely, Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) protocols. Evaluation of these routing protocols is performed based on the quantitative metrics such as Convergence Time, Jitter, End-to-End delay, Throughput and Packet Loss through the simulated network models. The evaluation results show that EIGRP routing protocol provides a better performance than OSPF routing protocol for real time applications. Through network simulations we have proved that EIGRP is more CPU intensive than OSPF and hence uses a lot of system power. Therefore EIGRP is a greener routing protocol and provides for greener internetworking.

50. Distributed Mobile Sink Routing for Wireless Sensor Networks: A Survey.

Synopsis:

The concentration of data traffic towards the sink in a wireless sensor network causes the nearby nodes to deplete their batteries quicker than other nodes, which leaves the sink stranded and disrupts the sensor data reporting. To mitigate this problem the usage of mobile sinks is proposed. Mobile sinks implicitly provide load-balancing and help achieving uniform energy-consumption across the network. However, the mechanisms to support the sink mobility (e.g., advertising the location of the mobile sink to the network) introduce an overhead in terms of energy consumption and packet delays. With these properties mobile sink routing constitutes an interesting research field with unique requirements. In this paper, we present a survey of the existing distributed mobile sink routing protocols. In order to provide an insight to the rationale and the concerns of a mobile sink routing protocol, design requirements and challenges associated with the problem of mobile sink routing are determined and explained. A definitive and detailed categorization is made and the protocols' advantages and drawbacks are determined with respect to their target applications.

51. Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks.

Synopsis:

Normally, authentication in vehicular ad-hoc networks (VANETs) uses Public Key Infrastructure (PKI) to verify the integrity of messages and the identity of message senders. The issues considered in the authentication schemes include the level of security and computational efficiency in verification processes. Most existing schemes focus mainly on assuring the security and privacy of VANET information. However, these schemes may not work well in VANET scenarios. For instance, it is difficult for a RoadSide Unit (RSU) to verify each vehicle’s signature sequentially when a large number of vehicles emerge in the coverage areas of an RSU. To reduce the computational overhead of RSUs, we propose a Proxy Based Authentication Scheme (PBAS) using distributed computing. In PBAS, proxy vehicles are used to authenticate multiple messages with a verification function at the same time. In addition, RSU is able to independently verify the outputs from the verification function of the proxy vehicles. We also design an expedite key negotiation scheme for transmitting sensitive messages. It is shown from the analysis and simulations that an RSU can verify 26500 signatures per second simultaneously with the help of the proxy vehicles. The time needed to verify 3000 signatures in PBAS can be reduced by 88% if compared to existing batch-based authentication schemes.

52. Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks.

Synopsis:

In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime.

53. Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks.

Synopsis:

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

54. A security-enhanced key authorization management scheme for trusted computing platform.

Synopsis:

Secure storage is one of the important functionalities in trusted computing platform. The key management is one of the important technologies in secure storage. There is a key synchronization problem in the existing trusted key authorization management mechanism for Trusted Computing Platform. To solve the problem, we propose a security-enhanced trusted key authorization management scheme. The new scheme can effectively enhance the trust and security of the trusted storage through adding child key information in parent key.

55. Assessing the veracity of identity assertions via OSNs.

Synopsis:

Anonymity is one of the main virtues of the Internet, as it protects privacy and enables users to express opinions more freely. However, anonymity hinders the assessment of the veracity of assertions that online users make about their identity attributes, such as age or profession. We propose FaceTrust, a system that uses online social networks to provide lightweight identity credentials while preserving a user's anonymity. Face-Trust employs a “game with a purpose” design to elicit the opinions of the friends of a user about the user's self-claimed identity attributes, and uses attack-resistant trust inference to assign veracity scores to identity attribute assertions. FaceTrust provides credentials, which a user can use to corroborate his assertions. We evaluate our proposal using a live Facebook deployment and simulations on a crawled social graph. The results show that our veracity scores strongly correlate with the ground truth, even when a large fraction of the social network users is dishonest and employs the Sybil attack.

56. Congestion Detection for Video Traffic in Wireless Sensor Networks.

Synopsis:

Congestion control mechanisms include three phases: congestion detection, congestion notification and rate adjustment. So far diverse congestion detection methods for sensor networks are proposed. In this paper we introduce numerous congestion detection parameters and examine them in various respects; finally we choose one of them as the best parameter for video traffic in wireless sensor networks. Some of intended criteria for comparing the parameters are cost, relation to quality of video, locality or being global in the network, accuracy and speed of congestion detection. We simulated and concluded that average delay is the most suitable parameter for congestion detection in these networks.

57. Continuous Neighbor Discovery in Asynchronous Sensor Networks.

Synopsis:

In most sensor networks, the nodes are static. Nevertheless, node connectivity is subject to changes because of disruptions in wireless communication, transmission power changes, or loss of synchronization between neighboring nodes. Hence, even after a sensor is aware of its immediate neighbors, it must continuously maintain its view, a process we call continuous neighbor discovery. In this work, we distinguish between neighbor discovery during sensor network initialization and continuous neighbor discovery. We focus on the latter and view it as a joint task of all the nodes in every connected segment. Each sensor employs a simple protocol in a coordinate effort to reduce power consumption without increasing the time required to detect hidden sensors.

58. Toward Privacy Preserving and Collusion Resistance in a Location Proof Updating System.

Synopsis:

Today's location-sensitive service relies on user's mobile device to determine the current location. This allows malicious users to access a restricted resource or provide bogus alibis by cheating on their locations. To address this issue, we propose A Privacy-Preserving LocAtion proof Updating System (APPLAUS) in which colocated Bluetooth enabled mobile devices mutually generate location proofs and send updates to a location proof server. Periodically changed pseudonyms are used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users evaluate their location privacy levels and decide whether and when to accept the location proof requests. In order to defend against colluding attacks, we also present betweenness ranking-based and correlation clustering-based approaches for outlier detection. APPLAUS can be implemented with existing network infrastructure, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost. Extensive experimental results show that APPLAUS can effectively provide location proofs, significantly preserve the source location privacy, and effectively detect colluding attacks.

59. Transfer Reliability and Congestion Control Strategies in Opportunistic Networks: A Survey.

Synopsis:

Opportunistic networks are a class of mobile ad hoc networks (MANETs) where contacts between mobile nodes occur unpredictably and where a complete end-to-end path between source and destination rarely exists at one time. Two important functions, traditionally provided by the transport layer, are ensuring the reliability of data transmission between source and destination, and ensuring that the network does not become congested with traffic. However, modified versions of TCP that have been proposed to support these functions in MANETs are ineffective in opportunistic networks. In addition, opportunistic networks require different approaches to those adopted in the more common intermittently connected networks, e.g. deep space networks. In this article we capture the state of the art of proposals for transfer reliability and storage congestion control strategies in opportunistic networks. We discuss potential mechanisms for transfer reliability service, i.e. hop-by-hop custody transfer and end-to-end return receipt. We also identify the requirements for storage congestion control and categorise these issues based on the number of message copies distributed in the networks. For single-copy forwarding, storage congestion management and congestion avoidance mechanism are discussed. For multiple-copy forwarding, the principal storage congestion control mechanisms are replication management and drop policy. Finally, we identify open research issues in the field where future research could usefully be focused.

60. Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection.

Synopsis:

Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. In this paper, we consider the problem of jamming-aware source routing in which the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. We formulate this traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. We show that in multisource networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). We demonstrate the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, we simulate the achievable throughput using our proposed traffic allocation method in several scenarios.

61. Live Streaming With Receiver-Based Peer-Division Multiplexing.

Synopsis:

A number of commercial peer-to-peer (P2P) systems for live streaming have been introduced in recent years. The behavior of these popular systems has been extensively studied in several measurement papers. Due to the proprietary nature of these commercial systems, however, these studies have to rely on a “black-box” approach, where packet traces are collected from a single or a limited number of measurement points, to infer various properties of traffic on the control and data planes. Although such studies are useful to compare different systems from the end-user's perspective, it is difficult to intuitively understand the observed properties without fully reverse-engineering the underlying systems. In this paper, we describe the network architecture of Zattoo, one of the largest production live streaming providers in Europe at the time of writing, and present a large-scale measurement study of Zattoo using data collected by the provider. To highlight, we found that even when the Zattoo system was heavily loaded with as high as 20 000 concurrent users on a single overlay, the median channel join delay remained less than 2-5 s, and that, for a majority of users, the streamed signal lags over-the-air broadcast signal by no more than 3 s.

62. Load-Balancing Multipath Switching System with Flow Slice.

Synopsis:

Multipath Switching systems (MPS) are intensely used in state-of-the-art core routers to provide terabit or even petabit switching capacity. One of the most intractable issues in designing MPS is how to load balance traffic across its multiple paths while not disturbing the intraflow packet orders. Previous packet-based solutions either suffer from delay penalties or lead to O(N^2) hardware complexity, hence do not scale. Flow-based hashing algorithms also perform badly due to the heavy-tailed flow-size distribution. In this paper, we develop a novel scheme, namely, Flow Slice (FS) that cuts off each flow into flow slices at every intraflow interval larger than a slicing threshold and balances the load on a finer granularity. Based on the studies of tens of real Internet traces, we show that setting a slicing threshold of 1-4 ms, the FS scheme achieves comparative load-balancing performance to the optimal one. It also limits the probability of out-of-order packets to a negligible level (10^{-6}) on three popular MPSes at the cost of little hardware complexity and an internal speedup up to two. These results are proven by theoretical analyses and also validated through trace-driven prototype simulations.

63. Optimal Power Allocation in Multi-Relay MIMO Cooperative Networks: Theory and Algorithms.

Synopsis:

Cooperative networking is known to have significant potential in increasing network capacity and transmission reliability. Although there have been extensive studies on applying cooperative networking in multi-hop ad hoc networks, most works are limited to the basic three-node relay scheme and single-antenna systems. These two limitations are interconnected and both are due to a limited theoretical understanding of the optimal power allocation structure in MIMO cooperative networks (MIMO-CN). In this paper, we study the structural properties of the optimal power allocation in MIMO-CN with per-node power constraints. More specifically, we show that the optimal power allocations at the source and each relay follow a matching structure in MIMO-CN. This result generalizes the power allocation result under the basic three-node setting to the multi-relay setting, for which the optimal power allocation structure has been heretofore unknown. We further quantify the performance gain due to cooperative relay and establish a connection between cooperative relay and pure relay. Finally, based on these structural insights, we reduce the MIMO-CN rate maximization problem to an equivalent scalar formulation. We then propose a global optimization method to solve this simplified and equivalent problem

64. NABS: Novel Approaches for Biometric Systems.

Synopsis:

Research on biometrics has noticeably increased. However, no single bodily or behavioral feature is able to satisfy acceptability, speed, and reliability constraints of authentication in real applications. The present trend is therefore toward multimodal systems. In this paper, we deal with some core issues related to the design of these systems and propose a novel modular framework, namely, novel approaches for biometric systems (NABS) that we have implemented to address them. NABS proposal encompasses two possible architectures based on the comparative speeds of the involved biometries. It also provides a novel solution for the data normalization problem, with the new quasi-linear sigmoid (QLS) normalization function. This function can overcome a number of common limitations, according to the presented experimental comparisons. A further contribution is the system response reliability (SRR) index to measure response confidence. Its theoretical definition allows to take into account the gallery composition at hand in assigning a system reliability measure on a single-response basis. The unified experimental setting aims at evaluating such aspects both separately and together, using face, ear, and fingerprint as test biometries. The results provide a positive feedback for the overall theoretical framework developed herein. Since NABS is designed to allow both a flexible choice of the adopted architecture, and a variable compositions and/or substitution of its optional modules, i.e., QLS and SRR, it can support different operational settings.

65. SPREAD: Improving network security by multipath routing in mobile ad hoc networks.

Synopsis:

We propose and investigate the SPREAD scheme as a complementary mechanism to enhance secure data delivery in a mobile ad hoc network. The basic idea is to transform a secret message into multiple shares, and then deliver the shares via multiple paths to the destination so that even if a certain number of message shares are compromised, the secret message as a whole is not compromised. We present the overall system architecture and discuss three major design issues: the mathematical model for the generation and reconstruction of the secret message shares, the optimal allocation of the message shares onto multiple paths in terms of security, and the multipath discovery techniques in a mobile ad hoc network. Our extensive simulation results justify the feasibility and the effectiveness of the SPREAD approach.

66. Reliability in Layered Networks With Random Link Failures.

Synopsis:

We consider network reliability in layered networks where the lower layer experiences random link failures. In layered networks, each failure at the lower layer may lead to multiple failures at the upper layer. We generalize the classical polynomial expression for network reliability to the multilayer setting. Using random sampling techniques, we develop polynomial-time approximation algorithms for the failure polynomial. Our approach gives an approximate expression for reliability as a function of the link failure probability, eliminating the need to resample for different values of the failure probability. Furthermore, it gives insight on how the routings of the logical topology on the physical topology impact network reliability. We show that maximizing the min cut of the (layered) network maximizes reliability in the low-failure-probability regime. Based on this observation, we develop algorithms for routing the logical topology to maximize reliability.

67. Self-Reconfigurable Wireless Mesh Networks..

Synopsis:

During their lifetime, multihop wireless mesh networks (WMNs) experience frequent link failures caused by channel interference, dynamic obstacles, and/or applications' bandwidth demands. These failures cause severe performance degradation in WMNs or require expensive manual network management for their real-time recovery. This paper presents an autonomous network reconfiguration system (ARS) that enables a multiradio WMN to autonomously recover from local link failures to preserve network performance. By using channel and radio diversities in WMNs, ARS generates necessary changes in local radio and channel assignments in order to recover from failures. Next, based on the thus-generated configuration changes, the system cooperatively reconfigures network settings among local mesh routers. ARS has been implemented and evaluated extensively on our IEEE 802.11-based WMN test-bed as well as through ns2-based simulation. Our evaluation results show that ARS outperforms existing failure-recovery schemes in improving channel-efficiency by more than 90% and in the ability of meeting the applications' bandwidth demands by an average of 200%.

68. Valuable Detours: Least-Cost Anypath Routing.

Synopsis:

In many networks, it is less costly to transmit a packet to any node in a set of neighbors than to one specific neighbor. This observation was previously exploited by opportunistic routing protocols by using single-path routing metrics to assign to each node a group of candidate relays for a particular destination. This paper addresses the least-cost anypath routing (LCAR) problem: how to assign a set of candidate relays at each node for a given destination such that the expected cost of forwarding a packet to the destination is minimized. The key is the following tradeoff: On one hand, increasing the number of candidate relays decreases the forwarding cost, but on the other, it increases the likelihood of “veering” away from the shortest-path route. Prior proposals based on single-path routing metrics or geographic coordinates do not explicitly consider this tradeoff and, as a result, do not always make optimal choices. The LCAR algorithm and its framework are general and can be applied to a variety of networks and cost models. We show how LCAR can incorporate different aspects of underlying coordination protocols, for example a link-layer protocol that randomly selects which receiving node will forward a packet, or the possibility that multiple nodes mistakenly forward a packet. In either case, the LCAR algorithm finds the optimal choice of candidate relays that takes into account these properties of the link layer. Finally, we apply LCAR to low-power, low-rate wireless communication and introduce a new wireless link-layer technique to decrease energy transmission costs in conjunction with anypath routing. Simulations show significant reductions in transmission cost to opportunistic routing using single-path metrics. Furthermore, LCAR routes are more robust and stable than those based on single-path distances due to the integrative nature of the LCAR's route cost metric.