Mobile computing for java/ dot net

1. Cloud-Assisted Mobile-Access of Health Data With Privacy and Auditability

Motivated by the privacy issues, curbing the adoption of electronic healthcare systems and the wild success of cloud service models, we propose to build privacy into mobile healthcare systems with the help of the private cloud. Our system offers salient features including efficient key management, privacy-preserving data storage, and retrieval, especially for retrieval at emergencies, and auditability for misusing health data. Specifically, we propose to integrate key management from pseudorandom number generator for unlinkability, a secure indexing method for privacy-preserving keyword search which hides both search and access patterns based on redundancy, and integrate the concept of attribute-based encryption with threshold signing for providing role-based access control with auditability to prevent potential misbehavior, in both normal and emergency cases.

2. A Scalable Server Architecture for Mobile Presence Services in Social Network Applications.

Synopsis:

Social network applications are becoming increasingly popular on mobile devices. A mobile presence service is an essential component of a social network application because it maintains each mobile user's presence information, such as the current status (online/offline), GPS location and network address, and also updates the user's online friends with the information continually. If presence updates occur frequently, the enormous number of messages distributed by presence servers may lead to a scalability problem in a large-scale mobile presence service. To address the problem, we propose an efficient and scalable server architecture, called PresenceCloud, which enables mobile presence services to support large-scale social network applications. When a mobile user joins a network, PresenceCloud searches for the presence of his/her friends and notifies them of his/her arrival. PresenceCloud organizes presence servers into a quorum-based server-to-server architecture for efficient presence searching. It also leverages a directed search algorithm and a one-hop caching strategy to achieve small constant search latency. We analyze the performance of PresenceCloud in terms of the search cost and search satisfaction level. The search cost is defined as the total number of messages generated by the presence server when a user arrives; and search satisfaction level is defined as the time it takes to search for the arriving user's friend list. The results of simulations demonstrate that PresenceCloud achieves performance gains in the search cost without compromising search satisfaction.

3. Fast Data Collection in Tree-Based Wireless Sensor Networks.

Synopsis:

We investigate the following fundamental question-how fast can information be collected from a wireless sensor network organized as tree? To address this, we explore and evaluate a number of different techniques using realistic simulation models under the many-to-one communication paradigm known as convergecast. We first consider time scheduling on a single frequency channel with the aim of minimizing the number of time slots required (schedule length) to complete a convergecast. Next, we combine scheduling with transmission power control to mitigate the effects of interference, and show that while power control helps in reducing the schedule length under a single frequency, scheduling transmissions using multiple frequencies is more efficient. We give lower bounds on the schedule length when interference is completely eliminated, and propose algorithms that achieve these bounds. We also evaluate the performance of various channel assignment methods and find empirically that for moderate size networks of about 100 nodes, the use of multifrequency scheduling can suffice to eliminate most of the interference. Then, the data collection rate no longer remains limited by interference but by the topology of the routing tree. To this end, we construct degree-constrained spanning trees and capacitated minimal spanning trees, and show significant improvement in scheduling performance over different deployment densities. Lastly, we evaluate the impact of different interference and channel models on the schedule length.

4. A Privacy-Preserving Location Monitoring System for Wireless Sensor Networks.

Synopsis:

Monitoring personal locations with a potentially untrusted server poses privacy threats to the monitored individuals. To this end, we propose a privacy-preserving location monitoring system for wireless sensor networks. In our system, we design two in-network location anonymization algorithms, namely, resource and quality-aware algorithms, that aim to enable the system to provide high-quality location monitoring services for system users, while preserving personal location privacy. Both algorithms rely on the well-established k-anonymity privacy concept, that is, a person is indistinguishable among k persons, to enable trusted sensor nodes to provide the aggregate location information of monitored persons for our system. Each aggregate location is in a form of a monitored area A along with the number of monitored persons residing in A, where A contains at least k persons. The resource-aware algorithm aims to minimize communication and computational cost, while the quality-aware algorithm aims to maximize the accuracy of the aggregate locations

by minimizing their monitored areas. To utilize the aggregate location information to provide location monitoring services, we use a spatial histogram approach that estimates the distribution of the monitored persons based on the gathered aggregate location information. Then, the estimated distribution is used to provide location monitoring services through answering range queries. We evaluate our system through simulated experiments. The results show that our system provides high-quality location monitoring services for system users and guarantees the location privacy of the monitored persons.

5. Efficient Authentication for Mobile and Pervasive Computing

Synopsis:

With today's technology, many applications rely on the existence of small devices that can exchange information and form communication networks. In a significant portion of such applications, the confidentiality and integrity of the communicated messages are of particular interest. In this work, we propose two novel techniques for authenticating short encrypted messages that are directed to meet the requirements of mobile and pervasive applications. By taking advantage of the fact that the message to be authenticated must also be encrypted, we propose provably secure authentication codes that are more efficient than any message authentication code in the literature. The key idea behind the proposed techniques is to utilize the security that the encryption algorithm can provide to design more efficient authentication mechanisms, as opposed to using standalone authentication primitives.

6. Community-Aware Opportunistic Routing in Mobile Social Networks.

Synopsis:

Mobile social networks (MSNs) are a kind of delay tolerant network that consists of lots of mobile nodes with social characteristics. Recently, many social-aware algorithms have been proposed to address routing problems in MSNs. However, these algorithms tend to forward messages to the nodes with locally optimal social characteristics, and thus cannot achieve the optimal performance. In this paper, we propose a distributed optimal Community-Aware Opportunistic Routing (CAOR) algorithm. Our main contributions are that we propose a home-aware community model, whereby we turn an MSN into a network that only includes community homes. We prove that, in the network of community homes, we can still compute the minimum expected delivery delays of nodes through a reverse Dijkstra

algorithm and achieve the optimal opportunistic routing performance. Since the number of communities is far less than the number of nodes in magnitude, the computational cost and maintenance cost of contact information are greatly reduced. We demonstrate how our algorithm significantly outperforms the previous ones through extensive simulations, based on a real MSN trace and a synthetic MSN trace.

7. Toward Reliable Data Delivery for Highly Dynamic Mobile Ad Hoc Networks.

Synopsis:

This paper addresses the problem of delivering data packets for highly dynamic mobile ad hoc networks in a reliable and timely manner. Most existing ad hoc routing protocols are susceptible to node mobility, especially for large-scale networks. Driven by this issue, we propose an efficient Position-based Opportunistic Routing (POR) protocol which takes advantage of the stateless property of geographic routing and the broadcast nature of wireless medium. When a data packet is sent out, some of the neighbor nodes that have overheard the transmission will serve as forwarding candidates, and take turn to forward the packet if it is not relayed by the specific best forwarder within a certain period of time. By utilizing such in-the-air backup, communication is maintained without being interrupted. The additional latency incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased. In the case of communication hole, a Virtual Destination-based Void Handling (VDVH) scheme is further proposed to work together with POR. Both theoretical analysis and simulation results show that POR achieves excellent performance even under high node mobility with acceptable overhead and the new void handling scheme also works well.

8. A Survey on Cluster-Based Group Key Agreement Protocols for WSNs.

Synopsis:

The scope of this survey is to examine and thoroughly evaluate the cluster-based Group Key Agreement (GKA) protocols for Wireless Sensor Networks (WSNs). Towards this goal, we have grouped the WSNs application environments into two major categories (i.e., infrastructure-based and infrastructureless) and have examined: a) which of the cluster-based Group Key Agreement (GKA) protocols that appear in the literature are applicable to each category, and b) to which degree these protocols will impact the systems' performance and energy consumption. In order to answer these questions we have calculated the complexity of each protocol and the energy cost it will add to the system. The evaluation of

all discussed protocols is presented in a generalized way and can therefore serve as a reference point for future evaluations and for the design of new, improved GKA protocols.

9. Preserving Location Privacy in Geosocial Applications.

Synopsis:

Using geosocial applications, such as FourSquare, millions of people interact with their surroundings through their friends and their recommendations. Without adequate privacy protection, however, these systems can be easily misused, for example, to track users or target them for home invasion. In this paper, we introduce LocX, a novel alternative that provides significantly improved location privacy without adding uncertainty into query results or relying on strong assumptions about server security. Our key insight is to apply secure user-specific, distance-preserving coordinate transformations to all location data shared with the server. The friends of a user share this user's secrets so they can apply the same transformation. This allows all location queries to be evaluated correctly by the server, but our privacy mechanisms guarantee that servers are unable to see or infer the actual location data from the transformed data or from the data access. We show that LocX provides privacy even against a powerful adversary model, and we use prototype measurements to show that it provides privacy with very little performance overhead, making it suitable for today's mobile devices.

10. Distributed Cooperative Caching in Social Wireless Networks.

Synopsis:

This paper introduces cooperative caching policies for minimizing electronic content provisioning cost in Social Wireless Networks (SWNET). SWNETs are formed by mobile devices, such as data enabled phones, electronic book readers etc., sharing common interests in electronic content, and physically gathering together in public places. Electronic object caching in such SWNETs are shown to be able to reduce the content provisioning cost which depends heavily on the service and pricing dependences among various stakeholders including content providers (CP), network service providers, and End Consumers (EC). Drawing motivation from Amazon's Kindle electronic book delivery business, this paper develops practical network, service, and pricing models which are then used for creating two object caching strategies for minimizing content provisioning costs in

networks with homogenous and heterogeneous object demands. The paper constructs analytical and simulation models for analyzing the proposed caching strategies in the presence of selfish users that deviate from network-wide cost-optimal policies. It also reports results from an Android phone-based prototype SWNET, validating the presented analytical and simulation results.

11. Adaptive Opportunistic Routing for Wireless Ad Hoc Networks.

Synopsis:

A distributed adaptive opportunistic routing scheme for multihop wireless ad hoc networks is proposed. The proposed scheme utilizes a reinforcement learning framework to opportunistically route the packets even in the absence of reliable knowledge about channel statistics and network model. This scheme is shown to be optimal with respect to an expected average per-packet reward criterion. The proposed routing scheme jointly addresses the issues of learning and routing in an opportunistic context, where the network structure is characterized by the transmission success probabilities. In particular, this learning framework leads to a stochastic routing scheme that optimally “explores” and “exploits” the opportunities in the network.

12. Secure High-Throughput Multicast Routing in Wireless Mesh Networks.

Synopsis:

Recent work in multicast routing for wireless mesh networks has focused on metrics that estimate link quality to maximize throughput. Nodes must collaborate in order to compute the path metric and forward data. The assumption that all nodes are honest and behave correctly during metric computation, propagation, and aggregation, as well as during data forwarding, leads to unexpected consequences in adversarial networks where compromised nodes act maliciously. In this work, we identify novel attacks against high-throughput multicast protocols in wireless mesh networks. The attacks exploit the local estimation and global aggregation of the metric to allow attackers to attract a large amount of traffic. We show that these attacks are very effective against multicast protocols based on high-throughput metrics. We conclude that aggressive path selection is a double-edged sword: While it maximizes throughput, it also increases attack effectiveness in the absence of defense mechanisms. Our approach to defend against the identified attacks combines measurement-based detection and accusation-based reaction techniques. The solution accommodates transient network variations and is resilient against attempts to exploit the defense mechanism itself. A detailed security analysis of our defense scheme establishes bounds on the impact of attacks. We demonstrate both the attacks

and our defense using ODMRP, a representative multicast protocol for wireless mesh networks, and SPP, an adaptation of the well-known ETX unicast metric to the multicast setting.

13. Privacy-Preserving Optimal Meeting Location Determination on Mobile Devices.

Synopsis:

Equipped with state-of-the-art smartphones and mobile devices, today's highly interconnected urban population is increasingly dependent on these gadgets to organize and plan their daily lives. These applications often rely on current (or preferred) locations of individual users or a group of users to provide the desired service, which jeopardizes their privacy; users do not necessarily want to reveal their current (or preferred) locations to the service provider or to other, possibly untrusted, users. In this paper, we propose privacy-preserving algorithms for determining an optimal meeting location for a group of users. We perform a thorough privacy evaluation by formally quantifying privacy-loss of the proposed approaches. In order to study the performance of our algorithms in a real deployment, we implement and test their execution efficiency on Nokia smartphones. By means of a targeted user-study, we attempt to get an insight into the privacy-awareness of users in location-based services and the usability of the proposed solutions.

14. Efficient Rekeying Framework for Secure Multicast with Diverse-Subscription-Period Mobile Users.

Synopsis:

Group key management (GKM) in mobile communication is important to enable access control for a group of users. A major issue in GKM is how to minimize the communication cost for group rekeying. To design the optimal GKM, researchers have assumed that all group members have the same leaving probabilities and that the tree is balanced and complete to simplify analysis. In the real mobile computing environment, however, these assumptions are impractical and may lead to a large gap between the impractical analysis and the measurement in real-life situations, thus allowing for GKM schemes to incorporate only a specific number of users. In this paper, we propose a new GKM framework supporting more general cases that do not require these assumptions. Our framework consists of two algorithms: one for initial construction of a basic key-tree and another for optimizing the key-tree after membership changes. The first algorithm enables the framework to generate an optimal key-tree that reflects the characteristics of users' leaving probabilities, and the second algorithm allows continual maintenance of communication with less overhead in group rekeying. Through simulations, we show that our GKM framework

outperforms the previous one which is known to be the best balanced and complete structure.

15. Supporting Efficient and Scalable Multicasting over Mobile Ad Hoc Networks.

Synopsis:

Group communications are important in Mobile Ad hoc Networks (MANETs). Multicast is an efficient method for implementing group communications. However, it is challenging to implement efficient and scalable multicast in MANET due to the difficulty in group membership management and multicast packet forwarding over a dynamic topology. We propose a novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a virtual-zone-based structure to implement scalable and efficient group membership management. A networkwide zone-based bidirectional tree is constructed to achieve more efficient membership management and multicast delivery. The position information is used to guide the zone structure building, multicast tree construction, and multicast packet forwarding, which efficiently reduces the overhead for route searching and tree structure maintenance. Several strategies have been proposed to further improve the efficiency of the protocol, for example, introducing the concept of zone depth for building an optimal tree structure and integrating the location search of group members with the hierarchical group membership management. Finally, we design a scheme to handle empty zone problem faced by most routing protocols using a zone structure. The scalability and the efficiency of EGMP are evaluated through simulations and quantitative analysis. Our simulation results demonstrate that EGMP has high packet delivery ratio, and low control overhead and multicast group joining delay under all test scenarios, and is scalable to both group size and network size. Compared to Scalable Position-Based Multicast (SPBM) [CHECK END OF SENTENCE], EGMP has significantly lower control overhead, data transmission overhead, and multicast group joining delay.

16. Video Dissemination over Hybrid Cellular and Ad Hoc Networks.

Synopsis:

We study the problem of disseminating videos to mobile users by using a hybrid cellular and ad hoc network. In particular, we formulate the problem of optimally choosing the mobile devices that will serve as gateways from the cellular to the ad hoc network, the ad hoc routes from the gateways to individual devices, and the layers to deliver on these ad hoc

routes. We develop a Mixed Integer Linear Program (MILP)-based algorithm, called POPT, to solve this optimization problem. We then develop a Linear Program (LP)-based algorithm, called MTS, for lower time complexity. While the MTS algorithm achieves close-to-optimum video quality and is more efficient than POPT in terms of time complexity, the MTS algorithm does not run in real time for hybrid networks with large numbers of nodes. We, therefore, propose a greedy algorithm, called THS, which runs in real time even for large hybrid networks. We conduct extensive packet-level simulations to compare the performance of the three proposed algorithms. We found that the THS algorithm always terminates in real time, yet achieves a similar video quality to MTS. Therefore, we recommend the THS algorithm for video dissemination over hybrid cellular and ad hoc networks.

17. Mobile Relay Configuration in Data-Intensive Wireless Sensor Networks.

Synopsis:

Wireless Sensor Networks (WSNs) are increasingly used in data-intensive applications such as microclimate monitoring, precision agriculture, and audio/video surveillance. A key challenge faced by data-intensive WSNs is to transmit all the data generated within an application's lifetime to the base station despite the fact that sensor nodes have limited power supplies. We propose using low-cost disposable mobile relays to reduce the energy consumption of data-intensive WSNs. Our approach differs from previous work in two main aspects. First, it does not require complex motion planning of mobile nodes, so it can be implemented on a number of low-cost mobile sensor platforms. Second, we integrate the energy consumption due to both mobility and wireless transmissions into a holistic optimization framework. Our framework consists of three main algorithms. The first algorithm computes an optimal routing tree assuming no nodes can move. The second algorithm improves the topology of the routing tree by greedily adding new nodes exploiting mobility of the newly added nodes. The third algorithm improves the routing tree by relocating its nodes without changing its topology. This iterative algorithm converges on the optimal position for each node given the constraint that the routing tree topology does not change. We present efficient distributed implementations for each algorithm that require only limited, localized synchronization. Because we do not necessarily compute an optimal topology, our final routing tree is not necessarily optimal. However, our simulation results show that our algorithms significantly outperform the best existing solutions.

18. Cut Detection in Wireless Sensor Networks.

Synopsis:

A wireless sensor network can get separated into multiple connected components due to the failure of some of its nodes, which is called a “cut.” In this paper, we consider the problem of detecting cuts by the remaining nodes of a wireless sensor network. We propose an algorithm that allows 1) every node to detect when the connectivity to a specially designated node has been lost, and 2) one or more nodes (that are connected to the special node after the cut) to detect the occurrence of the cut. The algorithm is distributed and asynchronous: every node needs to communicate with only those nodes that are within its communication range. The algorithm is based on the iterative computation of a fictitious “electrical potential” of the nodes. The convergence rate of the underlying iterative scheme is independent of the size and structure of the network. We demonstrate the effectiveness of the proposed algorithm through simulations and a real hardware implementation.

19. Throughput Optimization in Mobile Backbone Networks.

Synopsis:

This paper describes new algorithms for throughput optimization in a mobile backbone network. This hierarchical communication framework combines mobile backbone nodes, which have superior mobility and communication capability, with regular nodes, which are constrained in mobility and communication capability. An important quantity of interest in mobile backbone networks is the number of regular nodes that can be successfully assigned to mobile backbone nodes at a given throughput level. This paper develops a novel technique for maximizing this quantity in networks of fixed regular nodes using mixed-integer linear programming (MILP). The MILP-based algorithm provides a significant reduction in computation time compared to existing methods and is computationally tractable for problems of moderate size. An approximation algorithm is also developed that is appropriate for large-scale problems. This paper presents a theoretical performance guarantee for the approximation algorithm and also demonstrates its empirical performance. Finally, the mobile backbone network problem is extended to include mobile regular nodes, and exact and approximate solution algorithms are presented for this extension.

20. Privacy-Preserving Distributed Profile Matching in Proximity-Based Mobile Social Networks.

Synopsis:

Making new connections according to personal preferences is a crucial service in mobile social networking, where an initiating user can find matching users within physical proximity of him/her. In existing systems for such services, usually all the users directly publish their complete profiles for others to search. However, in many applications, the users' personal

profiles may contain sensitive information that they do not want to make public. In this paper, we propose FindU, a set of privacy-preserving profile matching schemes for proximity-based mobile social networks. In FindU, an initiating user can find from a group of users the one whose profile best matches with his/her; to limit the risk of privacy exposure, only necessary and minimal information about the private attributes of the participating users is exchanged. Two increasing levels of user privacy are defined, with decreasing amounts of revealed profile information. Leveraging secure multi-party computation (SMC) techniques, we propose novel protocols that realize each of the user privacy levels, which can also be personalized by the users. We provide formal security proofs and performance evaluation on our schemes, and show their advantages in both security and efficiency over state-of-the-art schemes.

21. Utility-Optimal Multi-Pattern Reuse in Multi-Cell Networks.

Synopsis:

Achieving sufficient spatial capacity gain through the use of small cells requires careful consideration of inter-cell interference (ICI) management via BS power coordination coupled with user scheduling inside cells. Optimal algorithms are known to be difficult to implement due to high computation and signaling overhead. This study proposes joint pattern-based ICI management and user scheduling algorithms that are practically implementable. The key idea is to decompose the original problem into two sub-problems in which ICI management is run at a slower time scale than user scheduling. We empirically show that even with such a slow tracking of system dynamics at the ICI management part, the decomposed approach achieves a considerable performance increase compared to conventional universal reuse schemes.

22. Wireless Sensor Network Security Model Using Zero Knowledge Protocol.

Synopsis:

Wireless Sensor Networks (WSNs) offer an excellent opportunity to monitor environments, and have a lot of interesting applications, some of which are quite sensitive in nature and require full proof secured environment. The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, we address some of the special security threats and attacks in WSNs. We propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack

is addressed by attaching a unique fingerprint to each node, that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The ZKP is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.

23. Search me if you can: Privacy-preserving location query service.

Synopsis:

Location-Based Service (LBS) becomes increasingly popular with the dramatic growth of smartphones and social network services (SNS), and its context-rich functionalities attract considerable users. Many LBS providers use users' location information to offer them convenience and useful functions. However, the LBS could greatly breach personal privacy because location itself contains much information. Hence, preserving location privacy while achieving utility from it is still an challenging question now. This paper tackles this non-trivial challenge by designing a suite of novel fine-grained Privacy-preserving Location Query Protocol (PLQP). Our protocol allows different levels of location query on encrypted location information for different users, and it is efficient enough to be applied in mobile platforms.

24. Self-Adaptive Contention Aware Routing Protocol for Intermittently Connected Mobile Networks.

Synopsis:

This paper introduces a novel multicopy routing protocol, called Self-Adaptive Utility-based Routing Protocol (SAURP), for Delay Tolerant Networks (DTNs) that are possibly composed of a vast number of devices in miniature such as smart phones of heterogeneous capacities in terms of energy resources and buffer spaces. SAURP is characterized by the ability of identifying potential opportunities for forwarding messages to their destinations via a novel utility function-based mechanism, in which a suite of environment parameters, such as wireless channel condition, nodal buffer occupancy, and encounter statistics, are jointly considered. Thus, SAURP can reroute messages around nodes experiencing high-buffer occupancy, wireless interference, and/or congestion, while taking a considerably small number of transmissions. The developed utility function in SAURP is proved to be able to achieve optimal performance, which is further analyzed via a stochastic modeling approach. Extensive simulations are conducted to verify the developed analytical model and compare the proposed SAURP with a number of recently reported encounter-based routing approaches in terms of delivery ratio, delivery delay, and the number of transmissions required for each message delivery. The simulation results show that SAURP outperforms all the counterpart multicopy encounter-based routing protocols considered in the study.

25. Toward a Statistical Framework for Source Anonymity in Sensor Networks.

Synopsis:

In certain applications, the locations of events reported by a sensor network need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such events by analyzing the network traffic. Known as the source anonymity problem, this problem has emerged as an important topic in the security of wireless sensor networks, with variety of techniques based on different adversarial assumptions being proposed. In this work, we present a new framework for modeling, analyzing, and evaluating anonymity in sensor networks. The novelty of the proposed framework is twofold: first, it introduces the notion of "interval indistinguishability" and provides a quantitative measure to model anonymity in wireless sensor networks; second, it maps source anonymity to the statistical problem of binary hypothesis testing with nuisance parameters. We then analyze existing solutions for designing anonymous sensor networks using the proposed model. We show how mapping source anonymity to binary hypothesis testing with nuisance parameters leads to converting the problem of exposing private source information into searching for an appropriate data transformation that removes or minimize the effect of the nuisance information. By doing so, we transform the problem from analyzing real-valued sample points to binary codes, which opens the door for coding theory to be incorporated into the study of anonymous sensor networks. Finally, we discuss how existing solutions can be modified to improve their anonymity.

26. Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks.

Synopsis:

Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-

concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

27. Keylogging-Resistant Visual Authentication Protocols

Synopsis:

The design of secure authentication protocols is quite challenging, considering that various kinds of root kits reside in Personal Computers (PCs) to observe user's behavior and to make PCs untrusted devices. Involving human in authentication protocols, while promising, is not easy because of their limited capability of computation and memorization. Therefore, relying on users to enhance security necessarily degrades the usability. On the other hand, relaxing assumptions and rigorous security design to improve the user experience can lead to security breaches that can harm the users' trust. In this paper, we demonstrate how careful visualization design can enhance not only the security but also the usability of authentication. To that end, we propose two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Through rigorous analysis, we verify that our protocols are immune to many of the challenging authentication attacks applicable in the literature. Furthermore, using an extensive case study on a prototype of our protocols, we highlight the potential of our approach for real-world deployment: we were able to achieve a high level of usability while satisfying stringent security requirements.

28. EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks.

Synopsis:

Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs) for their security. In any PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current CRL, and verifying the authenticity of the certificate and signature of the sender. In this paper, we propose an Expedite Message Authentication Protocol (EMAP) for VANETs, which replaces the time-consuming CRL checking process by an efficient revocation checking process. The revocation check process in EMAP uses a keyed Hash Message Authentication Code ({HMAC}), where the key used in calculating the {HMAC} is shared only between nonrevoked On-Board Units (OBUs). In addition, EMAP uses a novel probabilistic key distribution, which enables nonrevoked OBUs to securely share and update a secret key. EMAP can significantly decrease the message loss ratio due to the message verification delay compared with the conventional authentication methods

employing CRL. By conducting security analysis and performance evaluation, EMAP is demonstrated to be secure and efficient.

29. AMPLE: an adaptive traffic engineering system based on virtual routing topologies.

Synopsis:

Handling traffic dynamics in order to avoid network congestion and subsequent service disruptions is one of the key tasks performed by contemporary network management systems. Given the simple but rigid routing and forwarding functionalities in IP base environments, efficient resource management and control solutions against dynamic traffic conditions is still yet to be obtained. In this article, we introduce AMPLE - an efficient traffic engineering and management system that performs adaptive traffic control by using multiple virtualized routing topologies. The proposed system consists of two complementary components: offline link weight optimization that takes as input the physical network topology and tries to produce maximum routing path diversity across multiple virtual routing topologies for long term operation through the optimized setting of link weights. Based on these diverse paths, adaptive traffic control performs intelligent traffic splitting across individual routing topologies in reaction to the monitored network dynamics at short timescale. According to our evaluation with real network topologies and traffic traces, the proposed system is able to cope almost optimally with unpredicted traffic dynamics and, as such, it constitutes a new proposal for achieving better quality of service and overall network performance in IP networks.

30. A Spatiotemporal Approach for Secure Range Queries in Tiered Sensor Networks.

Synopsis:

We target a two-tier sensor network with resource-rich master nodes at the upper tier and resource-poor sensor nodes at the lower tier. Master nodes collect data from sensor nodes and answer the queries from the network owner. The reliance on master nodes for data storage and query processing raises serious concerns about both data confidentiality and query-result correctness in hostile environments. In particular, a compromised master node may leak hosted sensitive data to the adversary; it may also return juggled or incomplete data in response to a query. This paper presents a novel spatiotemporal approach to ensure secure range queries in event-driven two-tier sensor networks. It offers data confidentiality by preventing master nodes from reading hosted data and also enables efficient range-query processing. More importantly, it allows the network owner to verify with very high probability whether a query result is authentic and complete by examining the

spatial and temporal relationships among the returned data. The high efficacy and efficiency of our approach are confirmed by detailed performance evaluations.

31. Cooperative data dissemination via roadside WLANs

Synopsis:

Data dissemination services embrace a wide variety of telematic applications where data packets are generated at a remote server in the Internet and destined to a group of nomadic users such as vehicle passengers and pedestrians. The quality of a data dissemination service is highly dependent on the availability of network infrastructures in terms of the access points. In this article, we investigate the utilization of roadside wireless local area networks (RS-WLANs) as a network infrastructure for data dissemination. A two-level cooperative data dissemination approach is presented. With the network-level cooperation, the resources in the RS-WLANs are used to facilitate the data dissemination services for the nomadic users. The packet-level cooperation is exploited to improve the packet transmission rate to a nomadic user. Various techniques for the two levels of cooperation are discussed. A case study is presented to evaluate the performance of the data dissemination approach.

32. On Quality of Monitoring for Multichannel Wireless Infrastructure Networks.

Synopsis:

Passive monitoring utilizing distributed wireless sniffers is an effective technique to monitor activities in wireless infrastructure networks for fault diagnosis, resource management, and critical path analysis. In this paper, we introduce a quality of monitoring (QoM) metric defined by the expected number of active users monitored, and investigate the problem of maximizing QoM by judiciously assigning sniffers to channels based on the knowledge of user activities in a multichannel wireless network. Two types of capture models are considered. The user-centric model assumes the frame-level capturing capability of sniffers such that the activities of different users can be distinguished while the sniffer-centric model only utilizes the binary channel information (active or not) at a sniffer. For the user-centric model, we show that the implied optimization problem is NP-hard, but a constant approximation ratio can be attained via polynomial complexity algorithms. For the sniffer-centric model, we devise stochastic inference schemes to transform the problem into the user-centric domain, where we are able to apply our polynomial approximation algorithms. The effectiveness of our proposed schemes and algorithms is further evaluated using both synthetic data as well as real-world traces from an operational WLAN.

33.Converge-Cast: On the Capacity and Delay Tradeoffs.

Synopsis:

In this paper, we define an ad hoc network where multiple sources transmit packets to one destination as Converge-Cast network. We will study the capacity delay tradeoffs assuming that n wireless nodes are deployed in a unit square. For each session1, k nodes are randomly selected as active sources and transmit one packet to a particular destination node, which is also randomly selected. We first consider the stationary case, where capacity is mainly discussed and delay is entirely dependent on the average number of hops. We find that the per-node capacity is Θ (1/√n log n) 2, which is the same as that of unicast. Then node mobility is introduced to increase network capacity, for which our study is performed in two steps. The first step is to establish the delay in single-session transmission. We find that the delay is Θ (n log k) under 1-hop strategy and Θ (n log k/m) under 2-hop redundant strategy, where m denotes the number of replicas for each packet. The second step is to find delay and capacity in multisession transmission. We reveal that the per-node capacity and delay for 2-hop non-redundancy strategy are Θ (1) and Θ (n log k) respectively. The optimal delay is Θ (√n log k + k) with redundancy, corresponding to a capacity of Θ (root (1/n log k + k/n log k)). Therefore we obtain that the capacity delay tradeoff satisfies delay/rate ≥ Θ (n log k) for both strategies.

34. Network-Assisted Mobile Computing with Optimal Uplink Query Processing.

Synopsis:

Many mobile applications retrieve content from remote servers via user generated queries. Processing these queries is often needed before the desired content can be identified. Processing the request on the mobile devices can quickly sap the limited battery resources. Conversely, processing user queries at remote servers can have slow response times due communication latency incurred during transmission of the potentially large query. We evaluate a network-assisted mobile computing scenario where mid-network nodes with “leasing” capabilities are deployed by a service provider. Leasing computation power can reduce battery usage on the mobile devices and improve response times. However, borrowing processing power from mid-network nodes comes at a leasing cost which must be accounted for when making the decision of where processing should occur. We study the tradeoff between battery usage, processing and transmission latency, and mid-network leasing. We use the dynamic programming framework to solve for the optimal processing policies that suggest the amount of processing to be done at each mid-network node in

order to minimize the processing and communication latency and processing costs. Through numerical studies, we examine the properties of the optimal processing policy and the core tradeoffs in such systems.

35. Fast Release/Capture Sampling in Large-Scale Sensor Networks.

Synopsis:

Efficient estimation of global information is a common requirement for many wireless sensor network applications. Examples include counting the number of nodes alive in the network and measuring the scale of physically correlated events. These tasks must be accomplished at extremely low overhead due to the severe resource limitation of sensor nodes, which poses a challenge for large-scale sensor networks. In this paper, we develop a novel protocol FLAKE to efficiently and accurately estimate the global information of large-scale sensor networks based on the sparse sampling theory. Specially, FLAKE disseminates a small number of messages called seeds to the network and issues a query about which nodes receive a seed. The number of nodes that have the information of interest can be estimated by counting the seeds disseminated, the nodes queried, and the nodes that receive a seed. FLAKE can be easily implemented in a distributed manner due to its simplicity. Moreover, desirable tradeoffs can be achieved between the accuracy of estimation and the system overhead. Our simulations show that FLAKE significantly outperforms several existing schemes on accuracy, delay, and message overhead.

36. Optimal Multicast Capacity and DelayTradeoffs in MANETs.

Synopsis:

In this paper, we give a global perspective of multicast capacity and delay analysis in Mobile Ad Hoc Networks (MANETs). Specifically, we consider four node mobility models: (1) two-dimensional i.i.d. mobility, (2) two-dimensional hybrid random walk, (3) one-dimensional i.i.d. mobility, and (4) one-dimensional hybrid random walk. Two mobility time-scales are investigated in this paper: (i) fast mobility where node mobility is at the same time-scale as data transmissions and (ii) slow mobility where node mobility is assumed to occur at a much slower time-scale than data transmissions. Given a delay constraint D, we first characterize the optimal multicast capacity for each of the eight types of mobility models, and then we develop a scheme that can achieve a capacity-delay tradeoff close to the upper bound up to

a logarithmic factor. In addition, we also study heterogeneous networks with infrastructure support.

37. Topology control in mobile Ad Hoc networks with cooperative communications.

Synopsis:

Cooperative communication has received tremendous interest for wireless networks. Most existing works on cooperative communications are focused on link-level physical layer issues. Consequently, the impacts of cooperative communications on network-level upper layer issues, such as topology control, routing and network capacity, are largely ignored. In this article, we propose a Capacity-Optimized Cooperative (COCO) topology control scheme to improve the network capacity in MANETs by jointly considering both upper layer network capacity and physical layer cooperative communications. Through simulations, we show that physical layer cooperative communications have significant impacts on the network capacity, and the proposed topology control scheme can substantially improve the network capacity in MANETs with cooperative communications.

38.Protecting Location Privacy in Sensor Networks against a Global Eavesdropper.

Synopsis:

While many protocols for sensor network security provide confidentiality for the content of messages, contextual information usually remains exposed. Such contextual information can be exploited by an adversary to derive sensitive information such as the locations of monitored objects and data sinks in the field. Attacks on these components can significantly undermine any network application. Existing techniques defend the leakage of location information from a limited adversary who can only observe network traffic in a small region. However, a stronger adversary, the global eavesdropper, is realistic and can defeat these existing techniques. This paper first formalizes the location privacy issues in sensor networks under this strong adversary model and computes a lower bound on the communication overhead needed for achieving a given level of location privacy. The paper then proposes two techniques to provide location privacy to monitored objects (source-location privacy)-periodic collection and source simulation-and two techniques to provide location privacy to data sinks (sink-location privacy)-sink simulation and backbone flooding. These techniques provide trade-offs between privacy, communication cost, and latency. Through analysis and simulation, we demonstrate that the proposed techniques are efficient and effective for source and sink-location privacy in sensor networks.

39. Hop-by-Hop Routing in Wireless Mesh Networks with Bandwidth Guarantees.

Synopsis:

Wireless Mesh Network (WMN) has become an important edge network to provide Internet access to remote areas and wireless connections in a metropolitan scale. In this paper, we study the problem of identifying the maximum available bandwidth path, a fundamental issue in supporting quality-of-service in WMNs. Due to interference among links, bandwidth, a well-known bottleneck metric in wired networks, is neither concave nor additive in wireless networks. We propose a new path weight which captures the available path bandwidth information. We formally prove that our hop-by-hop routing protocol based on the new path weight satisfies the consistency and loop-freeness requirements. The consistency property guarantees that each node makes a proper packet forwarding decision, so that a data packet does traverse over the intended path. Our extensive simulation experiments also show that our proposed path weight outperforms existing path metrics in identifying high-throughput paths.

40.Optimal Content Downloading in Vehicular Networks

Synopsis:

We consider a system where users aboard communication-enabled vehicles are interested in downloading different contents from Internet-based servers. This scenario captures many of the infotainment services that vehicular communication is envisioned to enable, including news reporting, navigation maps, and software updating, or multimedia file downloading. In this paper, we outline the performance limits of such a vehicular content downloading system by modeling the downloading process as an optimization problem, and maximizing the overall system throughput. Our approach allows us to investigate the impact of different factors, such as the roadside infrastructure deployment, the vehicle-to-vehicle relaying, and the penetration rate of the communication technology, even in presence of large instances of the problem. Results highlight the existence of two operational regimes at different penetration rates and the importance of an efficient, yet 2-hop constrained, vehicle-to-vehicle relaying.

41. Data Delivery Properties of Human Contact Networks.

Synopsis:

Pocket Switched Networks take advantage of social contacts to opportunistically create data paths over time. This work employs empirical traces to examine the effect of the human contact process on data delivery in such networks. The contact occurrence distribution is found to be highly uneven: contacts between a few node pairs occur too

frequently, leading to inadequate mixing in the network, while the majority of contacts occur rarely, but are essential for global connectivity. This distribution of contacts leads to a significant variation in the fraction of node pairs that can be connected over time windows of similar duration. Good time windows tend to have a large clique of nodes that can all reach each other. It is shown that the clustering coefficient of the contact graph over a time window is a good predictor of achievable connectivity. We then examine all successful paths found by flooding and show that though delivery times vary widely, randomly sampling a small number of paths between each source and destination is sufficient to yield a delivery time distribution close to that of flooding over all paths. This result suggests that the rate at which the network can deliver data is remarkably robust to path failures.

42. Local Broadcast Algorithms in Wireless Ad Hoc Networks: Reducing the Number of Transmissions.

Synopsis:

There are two main approaches, static and dynamic, to broadcast algorithms in wireless ad hoc networks. In the static approach, local algorithms determine the status (forwarding/nonforwarding) of each node proactively based on local topology information and a globally known priority function. In this paper, we first show that local broadcast algorithms based on the static approach cannot achieve a good approximation factor to the optimum solution (an NP-hard problem). However, we show that a constant approximation factor is achievable if (relative) position information is available. In the dynamic approach, local algorithms determine the status of each node "on-the-fly" based on local topology information and broadcast state information. Using the dynamic approach, it was recently shown that local broadcast algorithms can achieve a constant approximation factor to the optimum solution when (approximate) position information is available. However, using position information can simplify the problem. Also, in some applications it may not be practical to have position information. Therefore, we wish to know whether local broadcast algorithms based on the dynamic approach can achieve a constant approximation factor without using position information. We answer this question in the positive-we design a local broadcast algorithm in which the status of each node is decided "on-the-fly" and prove that the algorithm can achieve both full delivery and a constant approximation to the optimum solution.

43. Distributed Adaptation of Quantized Feedback for Downlink Network MIMO Systems.

Synopsis:

This paper focuses on quantized channel state information (CSI) feedback for downlink network MIMO systems. Specifically, we propose to quantize and feedback the CSI of a subset of BSs, namely the feedback set. Our analysis reveals the tradeoff between better interference mitigation with large feedback set and high CSI quantization precision with small feedback set. Given the number of feedback bits and instantaneous/long-term channel conditions, each user optimizes its feedback set distributively according to the expected SINR derived from our analysis. Simulation results show that the proposed feedback adaptation scheme provides substantial performance gain over non-adaptive schemes, and is able to effectively exploit the benefits of network MIMO under various feedback bit budgets.

44. Minimum Bandwidth Reservations for Periodic Streams in Wireless Real-Time Systems.

Synopsis:

Reservation-based (as opposed to contention-based) channel access in WLANs provides predictable and deterministic transmission and is therefore able to provide timeliness guarantees for wireless and embedded real-time applications. Also, reservation-based channel access is energy-efficient since a wireless adaptor is powered on only during its exclusive channel access times. While scheduling for Quality of Service at the central authority (e.g., base station) has received extensive attention, the problem of determining the actual resource requirements of an individual node in a wireless real-time system has been largely ignored. This work aims at finding the minimum channel bandwidth reservation that meets the real-time constraints of all periodic streams of a given node. Keeping the bandwidth reservation of a node to a minimum leads to reduced energy and resource requirements and leaves more bandwidth for future reservations by other nodes. To obtain a solution to the minimum bandwidth reservation problem, we transform it to a generic uniprocessor task schedulability problem, which is then addressed using a generic algorithm. This algorithm works for a subclass of priority-driven packet scheduling policies, including three common ones: fixed-priority, EDF, and FIFO. Moreover, we then specialize the generic algorithm to these three policies according to their specific characteristics. Their computation complexities and bandwidth reservation efficiencies are evaluated and guidelines for choosing scheduling policies and stream parameters are presented.

45. Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure.

Synopsis:

Stealthy packet dropping is a suite of four attacks-misrouting, power control, identity delegation, and colluding collision-that can be easily launched against multihop wireless ad hoc networks. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node. However, the malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. Moreover, a legitimate node comes under suspicion. A popular method for detecting attacks in wireless networks is behavior-based detection performed by normal network nodes through overhearing the communication in their neighborhood. This leverages the open broadcast nature of wireless communication. An instantiation of this technology is local monitoring. We show that local monitoring, and the wider class of overhearing-based detection, cannot detect stealthy packet dropping attacks. Additionally, it mistakenly detects and isolates a legitimate node. We present a protocol called Sadec that can detect and isolate stealthy packet dropping attack efficiently. Sadec presents two techniques that can be overlaid on baseline local monitoring: having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor. Additionally, Sadec provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring. We show through analysis and simulation experiments that baseline local monitoring fails to efficiently mitigate most of the presented attacks while SADEC successfully mitigates them.

46. Throughput Optimization in High Speed Downlink Packet Access (HSDPA).

Synopsis:

In this paper, we investigate single user throughput optimization in High Speed Downlink Packet Access (HSDPA). Specifically, we propose offline and online optimization algorithms which adjust the Channel Quality Indicator (CQI) used by the network for scheduling of data transmission. In the offline algorithm, a given target block error rate (BLER) is achieved by adjusting CQI based on ACK/NAK history. By sweeping through different target BLERs, we can find the throughput optimal BLER offline. This algorithm could be used not only to optimize throughput but also to enable fair resource allocation among multiple users in HSDPA. In the online algorithm, the CQI offset is adapted using an estimated short term throughput gradient without the need for a target BLER. An adaptive stepsize mechanism is proposed to track temporal variation of the environment. Convergence behavior of both algorithms is analyzed. The part of the analysis that deals with constant step size gradient

algorithm may be applied to other stochastic optimization techniques. The convergence analysis is confirmed by our simulations. Simulation results also yield valuable insights on the value of optimal BLER target. Both offline and online algorithms are shown to yield up to 25% of throughput improvement over the conventional approach of targeting 10% BLER.