IEEE 2018-18 networking projects

An Enhanced Available Bandwidth Estimation technique for an End-to-End Network Path.

This paper presents a unique probing scheme, a rate adjustment algorithm, and a modified excursion detection algorithm (EDA) for estimating the available bandwidth (ABW) of an end-to-end network path more accurately and less intrusively. The proposed algorithm is based on the well-known concept of self-induced congestion and it features a unique probing train structure in which there is a region where packets are sampled more frequently than in other regions. This high-density region enables our algorithm to find the turning point more accurately. When the dynamic ABW is outside of this region, we readjust the lower rate and upper rate of the packet stream to fit the dynamic ABW into that region. We appropriately adjust the range between the lower rate and the upper rate using spread factors, which enables us to keep the number of packets low and we are thus able to measure the ABW less intrusively Available bandwidth (ABW) estimation is crucial for traffic engineering, quality-of-service (QoS) management, multimedia streaming, server selection in application services, congestion management, and network capacity provisioning in wireless mobile networks. ABW measurement can be considered essential to ensure that wireless mobile operators can achieve the QoS standard guaranteed by them while providing desired data rates to users. This can also be considered when comparing the performance index of various Telecom operators in a specific region.

Cost Minimization Algorithms for Data Center Management

Due to the increasing usage of cloud computing applications, it is important to minimize energy cost consumed by a data center, and simultaneously, to improve quality of service via data center management. One promising approach is to switch some servers in a data center to the idle mode for saving energy while to keep a suitable number of servers in the active mode for providing timely service. In this paper, we design both online and offline algorithms for this problem. For the offline algorithm, we formulate data center management as a cost minimization problem by considering energy cost, delay cost (to measure service quality), and switching cost (to change servers' active/idle mode). Then, we analyze certain properties of an optimal solution which lead to a dynamic programming based algorithm. Moreover, by revising the solution procedure, we successfully eliminate the recursive procedure and achieve an optimal offline algorithm with a polynomial complexity.

FRAPPE -Detecting Malicious Facebook Applications.

With 20 million installs a day, third-party apps are a major reason for the popularity and addictiveness of Facebook. Unfortunately, hackers have realized the potential of using apps for spreading malware and spam. The problem is already significant, as we find that at least 13% of apps in our dataset are malicious. So far, the research community has focused on detecting malicious posts and campaigns. In this paper, we ask the question: Given a Facebook application, can we determine if it is malicious? Our key contribution is in developing FRAppE—Facebook's Rigorous Application Evaluator—arguably the first tool focused on detecting malicious apps on Facebook. To develop FRAppE, we use information gathered by observing the posting behavior of 111K Facebook apps seen across 2.2 million users on Facebook. First, we identify a set of features that help us distinguishmalicious apps from beign ones. For example, we find that malicious apps often share names with other apps, and they typically request fewer permissions than benign apps. Second, leveraging these distinguishing features, we show that FRAppE can detect malicious apps with 99.5% accuracy, with no false positives and a high true positive rate (95.9%). Finally, we explore the ecosystem of malicious Facebook apps and identify mechanisms that these apps use to propagate.

JOKER: A Novel Opportunistic Routing Protocol

The increase in multimedia services has put energy saving on the top of current demands for mobile devices. Unfortunately, batteries' lifetime has not been as extended as it would be desirable. For that reason, reducing energy consumption in every task performed by these devices is crucial. In this work, a novel opportunistic routing protocol, called JOKER, is introduced. This proposal presents novelties in both the candidate selection and coordination phases, which permit increasing the performance of the network supporting multimedia traffic as well as enhancing the nodes' energy efficiency. JOKER is compared in different-nature test-benches with BATMAN routing protocol, showing its superiority in supporting a demanding service such as video-streaming in terms of QoE, while achieving a power draining reduction in routing tasks.

Multi-party secret key agreement over state-dependent wireless broadcast channels.

We consider a group of m trusted and authenticated nodes that aim to create a shared secret key K over a wireless channel in the presence of an eavesdropper Eve. We assume that there exists a state dependent wireless broadcast channel from one of the honest nodes to the rest of them including Eve. All of the trusted nodes can also discuss over a cost-free, noiseless and unlimited rate public channel which is also overheard by Eve. For this setup, we develop an information-theoretically secure

secret key agreement protocol. We show the optimality of this protocol for "linear deterministic" wireless broadcast channels. This model generalizes the packet erasure model studied in literature for wireless broadcast channels. Here, the main idea is to convert a deterministic channel to multiple independent erasure channels by using superposition coding. For "state-dependent Gaussian" wireless broadcast channels, by using insights from the deterministic problem, we propose an achievability scheme based on a multi-layer wiretap code. By using the wiretap code, we can mimic the phenomenon of converting the wireless channel to multiple independent erasure channels. Then, finding the best achievable secret key generation rate leads to solving a non-convex power allocation problem over these channels (layers). We show that using a dynamic programming algorithm, one can obtain the best power allocation for this problem. Moreover, we prove the optimality of the proposed achievability scheme for the regime of high-SNR and large-dynamic range over the channel states in the (generalized) degrees of freedom sense.

Optimizing Cloud-Service Performance: Efficient Resource Provisioning via Optimal Workload Allocation

The increase in multimedia services has put energy saving on the top of current demands for mobile devices. Unfortunately, batteries' lifetime has not been as extended as it would be desirable. For that reason, reducing energy consumption in every task performed by these devices is crucial. In this work, a novel opportunistic routing protocol, called JOKER, is introduced. This proposal presents novelties in both the candidate selection and coordination phases, which permit increasing the performance of the network supporting multimedia traffic as well as enhancing the nodes' energy efficiency. JOKER is compared in different-nature test-benches with BATMAN routing protocol, showing its superiority in supporting a demanding service such as video-streaming in terms of QoE, while achieving a power draining reduction in routing tasks.

PRISM Privacy-aware Interest Sharing and Matching in Mobile Social Networks.

In a profile matchmaking application of mobile social networks, users need to reveal their interests to each other in order to find the common interests. A malicious user may harm a user by knowing his personal information. Therefore, mutual interests need to be found in a privacy preserving manner. Here, we propose an efficient privacy protection and interests sharing protocol referred to as Privacy-aware Interest Sharing and Matching (PRISM). PRISM enables users to discover mutual interests without revealing their interests. Unlike existing approaches, PRISM does not require revealing the interests to a trusted server. The inherent mechanism reveals any cheating attempt by a malicious user. PRISM also proposes the procedure to eliminate Sybil attacks. We analyze the security of PRISM against both passive and active attacks. Through implementation, we also present a detailed analysis of the performance of PRISM and compare it with existing approaches. The results show the effectiveness of PRISM without any significant performance degradation.

Software Defined Networking with Pseudonym Systems for Secure Vehicular Clouds

The vehicular cloud is a promising new paradigm where vehicular networking and mobile cloud computing are elaborately integrated to enhance the quality of vehicular information services. Pseudonym is a resource for vehicles to protect their location privacy, which should be efficiently utilized to secure vehicular clouds. However, only a few existing architectures of pseudonym systems take flexibility and efficiency into consideration, thus leading to potential threats to location privacy. In this paper, we exploit software-defined networking technology to significantly extend the flexibility and programmability for pseudonym management in vehicular clouds. We propose a software-defined pseudonym system where the distributed pseudonym pools are promptly scheduled and elastically managed in a hierarchical manner. In order to decrease the system overhead due to the cost of inter-pool communications, we leverage the two-sided matching theory to formulate and solve the pseudonym resource scheduling. We conducted extensive simulations based on the real map of San Francisco. Numerical results indicate that the proposed software-defined pseudonym system significantly improves the pseudonym resource utilization, and meanwhile, effectively enhances the vehicles' location privacy by raising their entropy.

STAMP Enabling Privacy-Preserving Location Proofs for Mobile Users

Location-based services are quickly becoming immensely popular. In addition to services based on users' current location, many potential services rely on users' location history, or their spatial-temporal provenance. Malicious users may lie about their spatial-temporal provenance without a carefully designed security system for users to prove their past locations. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy.

Toward Optimum Crowdsensing Coverage With Guaranteed Performance.

Mobile crowdsensing networks have emerged to show elegant data collection capability in loosely cooperative network. However, in the sense of coverage quality, marginal works have considered the efficient (less participants) and effective (more coverage) designs for mobile crowdsensing network. We investigate the optimal coverage problem in distributed crowdsensing networks. In that, the sensing quality and the information delivery are jointly considered. Different from the conventional coverage problem, ours only select a subset of mobile users, so as to maximize the crowdsensing coverage with limited budget. We formulate our concerns as an optimal crowdsensing coverage problem, and prove its NP-completeness. In tackling this difficulty, we also prove the submodular property in our problem. Leveraging the favorable property in submodular optimization, we present the greedy algorithm with approximation ratio $O(\sqrt{k})$,where k is the number of selected users. Such that the information delivery and sensing coverage ratio could be guaranteed. Finally, we make extensive evaluations for the proposed scheme, with trace-driven tests. Evaluation results show that the proposed scheme could outperform the random selection by 2×with a random walk model, and over 3×with real trace data, in terms of crowdsensing coverage. Besides, the proposed scheme achieves near optimal solution comparing with the brute-force search results.

Vehicular Cloud Data Collection for Intelligent Transportation Systems.

The Internet of Things (IoT) envisions to connect billions of sensors to the Internet, in order to provide new applications and services for smart cities. IoT will allow the evolution of the Internet of Vehicles (IoV) from existing Vehicular Ad hoc Networks (VANETs), in which the delivery of various services will be offered to drivers by integrating vehicles, sensors, and mobile devices into a global network. To serve VANET with computational resources, Vehicular Cloud Computing (VCC) is recently envisioned with the objective of providing traffic solutions to improve our daily driving. These solutions involve applications and services for the benefit of Intelligent Transportation Systems (ITS), which represent an important part of IoV. Data collection is an important aspect in ITS, which can effectively serve online travel systems with the aid of Vehicular Cloud (VC). In this paper, we involve the new paradigm of VCC to propose a data collection model for the benefit of ITS. We show via simulation results that the participation of low percentage of vehicles in a dynamic VC is sufficient to provide meaningful data collection.