1. IEEE 2016: STAMP: Enabling Privacy-Preserving Location Proofs for Mobile Users

Abstract: 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.

2. IEEE 2016: Detecting Malicious Facebook Applications.

Abstract: 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 distinguish malicious apps from benign 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. Interestingly, we find that many apps collude and support each other; in our dataset, we find 1584 apps enabling the viral propagation of 3723 other apps through their posts. Long term, we see FRAppE as a step toward creating an independent watchdog for app assessment and ranking, so as to warn Facebook users before installing apps.

3. IEEE 2016: Toward Optimum Crowdsensing Coverage with Guaranteed Performance

Abstract: 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 effec-tive (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 sub modular property in our problem. Leveraging the favorable property in sub modular optimization, we present the greedy algorithm with approximation ratio $O(\sqrt{k})$,where 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.

4. IEEE 2016: PRISM: Privacy-aware Interest Sharing and Matching in Mobile Social Networks

Abstract: 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. In this paper, 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. Moreover, the protocol considers attacking scenarios that have not been addressed previously and provides an efficient solution. 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.

5. IEEE 2016: JOKER: A Novel Opportunistic Routing Protocol

Abstract: 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.

6. IEEE 2016: Software Defined Networking with Pseudonym Systems for Secure Vehicular Clouds

Abstract: The vehicular cloud is a promising new paradigm-m 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 ex-isting 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.

7. IEEE 2016: An Enhanced Available Bandwidth Estimation Technique for an End-to-End Network Path

Abstract: 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. Finally, to detect the ABW from the one-way queuing delay, we present a modified EDA from PathChirps' original EDA to better deal with sudden increase and decrease in queuing delays due to cross traffic burstiness. For the experiments, an Android OS-based device was used to measure the ABW over a commercial 4G/LTE mobile network of a Japanese mobile operator, as well as real test bed measurements were conducted over fixed and WLAN network. Simulations and experimental results show that our algorithm can achieve ABW estimations in real time and outperforms other state-of-the-art measurement algorithms in terms of accuracy, intrusiveness, and convergence time.

8. IEEE 2016: Privacy-Preserving Location Sharing Services for Social Networks

Abstract: A common functionality of many location-based social networking applications is a location sharing service that allows a group of friends to share their locations. With a potentially untrusted server, such allocation sharing service may threaten the privacy of users. Existing solutions for Privacy-Preserving Location Sharing Services (PPLSS) require a trusted third party that has access to the exact location of all users in the system or rely on expensive algorithms or protocols in terms of computational or communication overhead. Other solutions can only provide approximate query answers. To overcome these limitations, we propose a new encryption notion, called Order-Retrievable Encryption (ORE), for PPLSS for social networking applications. The distinguishing characteristics of our PPLSS are that it (1) allows a group of friends to share their exact locations without the need of any third party or leaking any location information to any server or users outside the group, (2) achieves low computational and communication cost by allowing users to receive the exact location of their friends without requiring any direct communication between users or multiple rounds of communication between a user and a server, (3) provides efficient query processing by designing an index structure for our ORE scheme, (4) supports dynamic location updates, and (5) provides personalized privacy protection within a group of friends by specifying a maximum distance where a user is willing to be located by his/her friends. Experimental

results show that the computational and communication cost of our PPLSS is much better than the state-of-the-art solution.

9. IEEE 2016: Authenticated Key Exchange Protocols for Parallel Network File Systems

Abstract: We study the problem of key establishment for secure many-to-many communications. The problem is inspired by the proliferation of large-scale distributed file systems supporting parallel access to multiple storage devices. Our work focuses on the current Internet standard for such file systems, i.e., parallel Network File System (pNFS), which makes use of Kerberos to establish parallel session keys between clients and storage devices. Our review of the existing Kerberos-based protocol shows that it has a number of limitations: (i) a metadata server facilitating key exchange between the clients and the storage devices has heavy workload that restricts the scalability of the protocol; (ii) the protocol does not provide forward secrecy; (iii) the metadata server generates itself all the session keys that are used between the clients and storage devices, and this inherently leads to key escrow. In this paper, we propose a variety of authenticated key exchange protocols that are designed to address the above issues. We show that our protocols are capable of reducing up to approximately 54 percent of the workload of the metadata server and concurrently supporting forward secrecy and escrow-freeness. All this requires only a small fraction of increased computation overhead at the client.

10. IEEE 2016: SmartCrawler: A Two-Stage Crawler for Efficiently Harvesting Deep-Web Interfaces

Abstract: As deep web grows at a very fast pace, there has been increased interest in techniques that help efficiently locate deep-web interfaces. However, due to the large volume of web resources and the dynamic nature of deep web, achieving wide coverage and high efficiency is a challenging issue. We propose a two-stage framework, namely SmartCrawler, for efficient harvesting deep web interfaces. In the first stage, SmartCrawler performs site-

based searching for center pages with the help of search engines, avoiding visiting a large number of pages. To achieve more accurate results for a focused crawl, SmartCrawler ranks websites to prioritize highly relevant ones for a given topic. In the second stage, SmartCrawler achieves fast in-site searching by excavating most relevant links with an adaptive link-ranking. To eliminate bias on visiting some highly relevant links in hidden web directories, we design a link tree data structure to achieve wider coverage for a website. Our experimental results on a set of representative domains show the agility and accuracy of our proposed crawler framework, which efficiently retrieves deep-web interfaces from large-scale sites and achieves higher harvest rates than other crawlers.

11. IEEE 2015: JAMMY: a Distributed and Self-Adaptive Solution against Selective Jamming Attack in TDMA WSNs

Abstract: Time Division Multiple Access (TDMA) is often used in Wireless Sensor Networks (WSNs), especially for critical applications, as it provides high energy efficiency, guaranteed bandwidth, bounded and predictable latency, and absence of collisions. However, TDMA is vulnerable to selective jamming attacks. In TDMA transmission, slots are typically pre-allocated to sensor nodes, and each slot is used by the same node for a number of consecutive super frames. Hence, an adversary could thwart a victim node's communication by simply jamming its slot(s). Such attack turns out to be effective, energy efficient, and extremely difficult to detect. In this paper, we present JAMMY, a distributed and dynamicsolution to selective jamming in TDMA-based WSNs. Unlike traditional approaches, JAMMY changes the slot utilization pattern at every super frame, thus making it unpredictable to the adversary. JAMMY is decentralized, as sensor nodes determine the next slot utilization pattern in a distributed and autonomous way. Results from performance analysis of the proposed solution show that JAMMY introduces negligible overhead yet allows multiple nodes to join the network, in a limited number of super frames.

12. IEEE 2015: Distortion-Aware Concurrent Multipath Transfer for Mobile Video Streaming in Heterogeneous Wireless Networks

Abstract: The massive proliferation of wireless infrastructures with complementary characteristics prompts the bandwidth aggregation for Concurrent Multipath Transfer (CMT) over heterogeneous access networks. Stream Control Transmission Protocol (SCTP) is the standard transport-layer solution to enable CMT in multi homed communication environments. However, delivering high-quality streaming video with the existing CMT solutions still remains problematic due to the stringent quality of service (QoS) requirements and path asymmetry in heterogeneous wireless networks. In this paper, we advance the state of the art by introducing video distortion into the decision process of multipath data transfer. The proposed distortion-aware concurrent multipath transfer (CMT-DA) solution includes three phases: 1) per-path status estimation and congestion control; 2) quality-optimal video flow rate allocation; 3) delay and loss controlled data retransmission. The term `flow rate allocation' indicates dynamically picking appropriate access networks and assigning the transmission rates. We analytically formulate the data distribution over multiple communication paths to minimize the end-to-end video distortion and derive the solution based on the utility maximization theory. The performance of the proposed CMT-DA is evaluated through extensive semi-physical emulations in Exata involving H.264 video streaming. Experimental results show that CMT-DA outperforms the reference schemes in terms of video peak signal-to-noise ratio (PSNR), good put, and inter-packet delay.

13.IEEE 2015: Cost-Effective Authentic and Anonymous Data Sharing with Forward Security

Abstract: Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows

a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to re authenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

14.IEEE 2015: SHARP: Secured Hierarchical Anonymous Routing Protocol for MANETs

Abstract: Mobile ad-hoc network (MANET) is one of the developing fields for research and development of wireless network. MANETs are self-organizing, infrastructure less, independent, dynamic topology based, open and decentralized networks. This is an ideal choice for uses such as communication and data sharing. Due to the open and decentralized nature of the network the nodes can join or leave the network as they wish. There is no centralized authority to maintain the membership of nodes in the network. In MANETs security is the major concern in applications such as communication and data sharing. These are so many chances of different types of attacks due to self- organizing property of MANETs. Malicious attacker may try to attack the data packets by tracing the route. They may try to find the source and destination through different types attacks. MANETs are vulnerable to malicious attackers that target to damage and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing protocols are used by MANETs that hides the identity of nodes as well as routes from outside observers. In MANETs anonymity means identity and location anonymity of data sources and destinations as well as route anonymity.

However existing anonymous routing protocols have significantly high cost, which worsens the resource constraint problem in MANETs. This paper proposes Secured Hierarchical Anonymous Routing Protocol (SHARP) based on cluster routing. SHARP offers anonymity to source, destination, and routes. Theoretically SHARP achieves better anonymity protection compared to other anonymous routing protocols.

15. IEEE 2015: CStream: Neighborhood Bandwidth Aggregation for Better Video Streaming

Abstract: Despite the popularity of watching videos online, challenges still remain in video streaming in many scenarios. Limited home broadband and mobile phone 3G bandwidths mean many users stream videos at compromised quality. To provide additional bandwidth for streaming, we propose CStream, a system that aggregates bandwidth from multiple cooperating users in a neighborhood environment for better video streaming. CStream exploits the fact that wireless devices have multiple network interfaces and connects cooperating users with a wireless ad-hoc network to aggregate their unused downlink Inter- net bandwidth. CStream dynamically generates a streaming plan to stream a single video using multiple connections, continuously adapting to changes in the neighborhood and variations in the available band- width. CStream is developed and evaluated on a test bed of computers, allowing for a detailed, controlled evaluation of performance. Analysis of the results shows a linear increase in throughput over single- connection streaming and improved video quality as the number of cooperating users in a neighborhood increase.

16. IEEE 2015: The Mason Test: A Defense Against Sybil Attacks in Wireless Networks Without Trusted Authorities

Abstract: Wireless networks are vulnerable to Sybil attacks, in which a malicious node poses as many identities in order to gain disproportionate influence. Many defenses based on spatial variability of wireless channels exist, but depend either on detailed, multi-tap channel

estimation-something not exposed on commodity 802.11 devices-or valid RSSI observations from multiple trusted sources, e.g., corporate access points-something not directly available in ad hoc and delay-tolerant networks with potentially malicious neighbors. We extend these techniques to be practical for wireless ad hoc networks of commodity 802.11 devices. Specifically, we propose two efficient methods for separating the valid RSSI observations of behaving nodes from those falsified by malicious participants. Further, we note that prior signal print methods are easily defeated by mobile attackers and develop an appropriate challenge-response defense. Finally, we present the Mason test, the first implementation of these techniques for ad hoc and delay-tolerant networks of commodity 802.11 devices. We illustrate its performance in several real-world scenarios.

17. IEEE 2015: Passive IP Traceback: Disclosing the Locations of IP Spoofers From Path Backscatter

Abstract: It is long known attackers may use forged source IP address to conceal their real locations. To capture the spoofers, a number of IP traceback mechanisms have been proposed. However, due to the challenges of deployment, there has been not a widely adopted IP traceback solution, at least at the Internet level. As a result, the mist on the locations of spoofers has never been dissipated till now. This paper proposes passive IP traceback (PIT) that bypasses the deployment difficulties of IP traceback techniques. PIT investigates Internet Control Message Protocol error messages (named path backscatter) triggered by spoofing traffic, and tracks the spoofers based on public available information (e.g., topology). In this way, PIT can find the spoofers without any deployment requirement. This paper illustrates the causes, collection, and the statistical results on path backscatter, demonstrates the processes and effectiveness of PIT, and shows the captured locations of spoofers through applying PIT on the path backscatter data set. These results can help further reveal IP spoofing, which has been studied for long but never well understood. Though PIT cannot work in all the spoofing attacks, it may be the most useful mechanism to trace spoofers before an Internet-level traceback system has been deployed in real.

18. IEEE 2015: Resource Allocation for Energy Efficiency Optimization in Heterogeneous Networks

Abstract: Heterogeneous network (HetNet) deployment is considered a de facto solution for meeting the ever increasing mobile traffic demand. However, excessive power usage in such networks is a critical issue, particularly for mobile operators. Characterizing the fundamental energy efficiency (EE) performance of HetNets is therefore important for the design of green wireless systems. In this paper, we address the EE optimization problem for downlink two-tier HetNets comprised of a single macro-cell and multiple pico-cells. Considering a heterogeneous real-time and non-real-time traffic, transmit be am forming design and power allocation policies are jointly considered in order to optimize the system energy efficiency. The EE resource allocation problem under consideration is a mixed combinatorial and non-convex optimization problem, which is extremely difficult to solve. In order to reduce the computational complexity, we decompose the original problem with multiple inequality constraints into multiple optimization problems with single inequality constraint. For the latter problem, a two-layer resource allocation algorithm is proposed based on the quasiconcavity property of EE. Simulation results confirm the theoretical findings and demonstrate that the proposed resource allocation algorithm can efficiently approach the optimal EE.

19. IEEE 2015: A Distributed Three-Hop Routing Protocol to Increase the Capacity of Hybrid Wireless Networks

Abstract: Hybrid wireless networks combining the advantages of both mobile ad-hoc networks and infrastructure wireless networks have been receiving increased attention due to their ultra-high performance. An efficient data routing protocol is important in such networks for high network capacity and scalability. However, most routing protocols for these networks simply combine the ad-hoc transmission mode with the cellular transmission mode, which inherits the drawbacks of ad-hoc transmission. This paper presents a Distributed Three-hop Routing protocol (DTR) for hybrid wireless networks. To take full advantage of the widespread base stations, DTR divides a message data stream into segments

and transmits the segments in a distributed manner. It makes full spatial reuse of a system via its high speed ad-hoc interface and alleviates mobile gateway congestion via its cellular interface. Furthermore, sending segments to a number of base stations simultaneously increases throughput and makes full use of widespread base stations. In addition, DTR significantly reduces overhead due to short path lengths and the elimination of route discovery and maintenance. DTR also has a congestion control algorithm to avoid overloading base stations. Theoretical analysis and simulation results show the superiority of DTR in comparison with other routing protocols in terms of throughput capacity, scalability, and mobility resilience. The results also show the effectiveness of the congestion control algorithm in balancing the load between base stations.

20. IEEE 2015: A Computational Dynamic Trust Model for User Authorization

Abstract: Development of authorization mechanisms for secure information access by a large community of users in an open environment is an important problem in the ever-growing Internet world. In this paper we propose a computational dynamic trust model for user authorization, rooted in findings from social science. Unlike most existing computational trust models, this model distinguishes trusting belief in integrity from that in competence in different contexts and accounts for subjectivity in the evaluation of a particular trustee by different thrusters. Simulation studies were conducted to compare the performance of the proposed integrity belief model with other trust models from the literature for different user behavior patterns. Experiments show that the proposed model achieves higher performance than other models especially in predicting the behavior of unstable users.

21. IEEE 2015: Generating Searchable Public-Key Ciphertexts with Hidden Structures for Fast Keyword Search

Abstract: Existing semantically secure public-key searchable encryption schemes take search time linear with the total number of the ciphertexts. This makes retrieval from large-scale databases prohibitive. To alleviate this problem, this paper

proposes searchable public-key ciphertexts with hidden structures (SPCHS) for keyword search as fast as possible without sacrificing semantic security of the encrypted keywords. In SPCHS, all keyword-searchable ciphertexts are structured by hidden relations, and with the search trapdoor corresponding to a keyword, the minimum information of the relations is disclosed to a search algorithm as the guidance to find all matching ciphertexts efficiently. We construct an SPCHS scheme from scratch in which the ciphertexts have a hidden star-like structure. We prove our scheme to be semantically secure in the random oracle (RO) model. The search complexity of our scheme is dependent on the actual number of the ciphertexts containing the queried keyword, rather than the number of all ciphertexts. Finally, we present a generic SPCHS construction from anonymous identity-based encryption and collision-free full-identity malleable identity-based key encapsulation mechanism (IBKEM) with anonymity. We illustrate two collision-free full-identity malleable IBKEM instances, which are semantically secure and anonymous, respectively, in the RO and standard models. The latter instance enables us to construct an SPCHS scheme with semantic security in the standard model.

22. IEEE 2015: A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet DropAttacks in Wireless Sensor Networks

Abstract: Large-scale sensor networks are deployed in numerous application domains, and the data they collect are used in decision-making for critical infrastructures. Data are streamed from multiple sources through intermediate processing nodes that aggregate information. A malicious adversary may introduce additional nodes in the network or compromise existing ones. Therefore, assuring high data trustworthiness is crucial for correct decision-making. Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. In this paper, we propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification

and reconstruction at the base station. In addition, we extend the secure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes. We evaluate the proposed technique both analytically and empirically, and the results prove the effectiveness and efficiency of the lightweightsecure provenance scheme in detecting packet forgery and loss attacks.