SCANNING THE LITERATURE

EDITED BY PAN LI

DOF: A Local Wireless Information Plane

Steven Hong and Sachin Katti, ACM SIGCOMM, Toronto, ON, Canada, August 2011

The ability to detect which unlicensed radios are operating in a neighborhood, their spectrum occupancies, and the spatial directions their signals are traversing is a fundamental primitive needed by many applications, ranging from smart radios to coexistence to network management to security. This paper presents DOF, a detector that in a single framework accurately estimates all three parameters. DOF builds on the insight that in most wireless protocols, there are hidden repeating patterns in the signals that can be used to construct unique signatures, and accurately estimate signal types and their spectral and spatial parameters. The paper shows via experimental evaluation in an indoor testbed that DOF is robust and accurate, and achieves greater than 85 percent accuracy even when the signal-to-noise ratios (SNRs) of the detected signals are as low as 0 dB, and even when there are multiple interfering signals present. To demonstrate the benefits of DOF, the authors design and implement a preliminary prototype of a smart radio that operates on top of DOF, and show experimentally that it provides a 80 percent increase in throughput over Jello, the best known prior implementation, while causing less than 10 percent performance drop for co-existing WiFi and Zigbee radios.

No Time to Countdown: Migrating Backoff to the Frequency Domain

Souvik Sen, Romit Roy Choudhury, and Srihari Nelakuditi, ACM MobiCom, Las Vegas, NV, USA, September 2011

Conventional WiFi networks perform channel contention in the time domain. This is known to be wasteful because the channel is forced to remain idle while all contending nodes are backing off for multiple time slots. This paper proposes to break away from convention and recreate the backing off operation in the frequency domain. The basic idea leverages the observation that OFDM subcarriers can be treated as integer numbers. Thus, instead of picking a random backoff duration in time, a contending node can signal on a randomly chosen subcarrier. By employing a second antenna to listen to all the subcarriers, each node can determine whether its chosen integer (or subcarrier) is the smallest among all others. In fact, each node can even determine the rank of its chosen subcarrier, enabling the feasibility of scheduled transmissions after every round of contention. The authors develop these ideas into a Back2F protocol that migrates WiFi backoff to the frequency domain. Experiments on a prototype of 10 USRPs confirm feasibility, along with consistent throughput gains over 802.11. Trace based simulations affirm scalability to larger, real-world network topologies.

PACP: An Efficient Pseudonymous Authentication-Based Conditional Privacy Protocol for VANETs

Dijiang Huang, Satyajayant Misra, Mayank Verma, and Guoliang Xue, IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 3, September 2011, pp. 736–46

This paper proposes a new privacy preservation scheme, named pseudonymous authentication-based conditional privacy (PACP), which allows vehicles in a vehicular ad hoc network (VANET) to use pseudonyms instead of their true identity to obtain provably good privacy. In the proposed scheme, vehicles interact with roadside units to help them generate pseudonyms for anonymous communication. In the scheme setup, the pseudonyms are only known to the vehicles but have no other entities in the network. In addition, the proposed scheme provides an efficient revocation mechanism that allows vehicles to be identified and revoked from the network if needed. Thus, the authors can provide conditional privacy to the vehicles in the system, that is, the vehicles will be anonymous in the network until they are revoked, at which point, they cease to be anonymous.

Achieving MAC-Layer Fairness in CSMA/CA Networks

Ying Jian, Ming Zhang, and Shigang Chen, IEEE/ACM Transactions on Networking, vol. 19, no. 5, October 2011, pp. 1472–84

CSMA/CA networks, including IEEE 802.11 networks, exhibit severe fairness problem in many scenarios, where some hosts obtain most of the channel's bandwidth while others starve. Most existing solutions require nodes to overhear transmissions made by contending nodes and, based on the overheard information, adjust local rates to achieve fairness among all contending links. Their underlying assumption is that transmissions made by contending nodes can be overheard. However, this assumption holds only when the transmission range is equal to the interference range, which is not true in reality. As this paper reveals, the overhearing-based solutions, as well as several nonoverhearing AIMD solutions, cannot achieve MAC-layer fairness in various settings. The authors propose a new rate control protocol, called Proportional Increase Synchronized multiplicative Decrease (PISD). Without relying on overhearing, it provides fairness in CSMA/CA networks, particularly IEEE 802.11 networks, by using only local information and performing localized operations. It combines several novel rate control mechanisms, including synchronized multiplicative decrease, proportional increase, and background transmission. The authors prove that PISD converges and achieves (weighted) fairness. They further introduce Queue Spreading (QS) to achieve MAC-layer fairness when there are multiple contention groups, in which case PISD will fail.

Interference Channel with Constrained Partial Group Decoding

Chen Gong, Ali Tajer, and Xiaodong Wang, IEEE Transactions on Communications, vol. 59, no. 11, November 2011, pp. 3059–71

This paper proposes novel coding and decoding methods for a fully connected K-user Gaussian interference channel. Each transmitter encodes its information into multiple layers and transmits the superposition of those layers. Each receiver employs a constrained partial group decoder (CPGD) that decodes its designated message along with a part of the interference. In particular, each receiver performs a twofold task by first identifying which interferers it should decode and then determining which layers of them should be decoded. Determining the layers to be decoded and decoding them are carried out in a successive manner, where in each step a group of layers with a constraint on its group size is identified and jointly decoded while the remaining layers are treated as Gaussian noise. The decoded layers are then subtracted from the received signal, and the same procedure is repeated for the remaining layers. The authors provide a distributed algorithm, tailored to the nature of the interference channels, that determines the transmission rate at each transmitter based on some optimality measure and also finds the order of the layers to be successively decoded at each receiver. They also consider practical design of a system that employs quadrature amplitude modulations (QAM) and rateless codes. Numerical results are provided on the achievable sum-rate under the ideal case of Gaussian signaling with random codes as well as on the system throughput under practical modulations and channel codes. The results show that the proposed multilayer coding scheme with CPGD offers significant performance gain over traditional unlayered transmission with single-user decoding.

Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs

Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, and Xuemin (Sherman) Shen, IEEE Transactions on Vehicular Technology, vol. 61, no. 1, January 2012, pp. 86–96

As a prime target of quality of privacy (QoP) in vehicular ad hoc networks (VANETs), location privacy is imperative for the full flourish of VANETs. Although frequent pseudonym changing provides a promising solution for location privacy in VANETs, if the pseudonyms are changed in an improper time or location, such a solution may become invalid. To cope with the issue, this paper presents an effective pseudonym changing at social spots (PCS) strategy to achieve the provable location privacy. Specifically, the authors first introduce the social spots where many vehicles may gather, such as a road intersection when the traffic light turns red or a free parking lot near a shopping mall. By taking the anonymity set size (ASS) as the location privacy metric, they then develop two anonymity set analytic models to quantitatively investigate the location privacy achieved by the PCS strategy. In addition, the authors use game theoretic techniques to prove the feasibility of PCS strategy in practice. Extensive performance evaluations are conducted to demonstrate that better location privacy can be achieved when a vehicle changes its pseudonyms at some highly social spots, and the proposed PCS strategy can assist vehicles to intelligently change their pseudonyms at the right moment and place.