Prize Winners’ Talks

Data Transfer Using a Camera and a Three-Dimensional Code

Jeton Memeti
University of Zurich

Abstract:
One- and two-dimensional barcodes have become very popular in past years and are widely used to identify products as well as services. Recently, 2D barcodes, like QR codes, are also used to transfer optically a dedicated hyperlink. All 2D barcodes share one major weakness: the storage capacity. To overcome that, time can be introduced as a third dimension. Instead of one, a sequence of barcodes is used to transfer a larger amount of data. The main goal of the present work was to design, implement, and especially evaluate the entire workflow for such a QR code-based, three-dimensional (3D) transmission system on the receiver side, such as a Smartphone, being able to “read” from a sender, represented by a screen. The steps comprise the capturing of the 3D barcode, the recognition and reading of the sequence of 2D barcodes, and the final retrieval of the original content. Furthermore, adversarial conditions had to be identified, tested, and documented in detail. The prototype achieves a theoretical throughput of 12,288 Byte for 30 seconds transmission intervals, which results in approximately 3,280 bit/s. Future work may focus on increasing the throughput of the system as well as the transmission reliability by applying error detection and correction techniques.
Prize Winners’ Talks

Implementation of the HIP Diet Exchange and Optimizations for Smart Object Networks

Jens Hiller
RWTH Aachen University

Abstract:
Today, lightweight IP stacks enable smart objects to exchange information with each other as well as with backend services over the Internet. To protect the confidentiality and integrity of data that is gathered by smart objects in industrial monitoring or e-health systems, the communicating peers need to authenticate each other and encrypt the transmitted data. However, security protocols must cope with the constrained resources of smart objects that only offer a few KB of RAM and ROM, are equipped with CPUs of a few MHz and often are battery-powered. In this article, we provide a brief overview and analysis of the IP security protocols DTLS, Minimal IKE, and HIP DEX. We then present our optimization for the HIP DEX DoS protection mechanism and hint at further improvements that are discussed in the thesis this article is based on. Finally, we provide a detailed overhead evaluation of HIP DEX based on our own implementation.
Prize Winners’ Talks

Socio- and Locality-Aware Overlays for User-Centric Networking

Martin Florian
Karlsruher Institute of Technology

Abstract:
Online social networks and socially motivated communication in general are as much a modern trend as the ubiquity and growing capability of mobile consumer devices like smartphones. Based on these trends, user-centric networking can be realized directly between user devices, i.e. without depending on a server-based infrastructure. Moving towards this vision, the SODESSON project aims at developing a generic user-centric networking middleware for the easy development of decentralized user-centric applications. The goal of the presented thesis was the exploration of a suitable base for such a middleware. Following an extensive analysis of possible approaches, a fully decentralized, overlay-based publish/subscribe system was proposed that maximizes communication locality and leverages social connections between users to improve the performance of the system and enable the deployment of novel socio-aware services. The presented approach supports the persistence and delayed delivery of messages to temporarily unreachable recipients and does not depend on permanent Internet connectivity. The design was evaluated using the OverSim simulation framework, which was modified to support the simulation of user-centric networking scenarios. Results show that the approach achieves close to optimal latencies and scales well with growing network sizes.
Prize Winners’ Talks

Traffic-Adaptive and Link-Quality-Aware Communication in Wireless Sensor Networks

Philipp Hurni
University of Bern

Abstract:

The main research contributions of this doctoral thesis are driven by the research question how to design simple, yet efficient and robust run-time adaptive resource allocation schemes within the communication stack of Wireless Sensor Network (WSN) nodes. The thesis addresses several problem domains with contributions on different layers of the WSN communication stack. The main contributions can be summarized as follows: First, a novel run-time adaptive MAC protocol is introduced, which stepwise allocates the power-hungry radio interface in an on-demand manner when the encountered traffic load requires it. Second, the thesis outlines a methodology for robust, reliable and accurate software-based energy-estimation, which is calculated at network run-time on the sensor node itself. Third, the thesis evaluates several Forward Error Correction (FEC) strategies to adaptively allocate the correctional power of Error Correcting Codes (ECCs) to cope with timely and spatially variable bit error rates. Fourth, in the context of TCP-based communications in WSNs, the thesis evaluates distributed caching and local retransmission strategies to overcome the performance degrading effects of packet corruption and transmission failures when transmitting data over multiple hops. All of the developed protocol's performances are evaluated in a self-developed real-world WSN testbed and achieve superior performance over selected existing approaches, especially where traffic load and channel conditions are suspect to rapid variations over time.
Prize Winners’ Talks

Direct End-to-Middle Authentication in Cooperative Networks

Tobias Heer
RWTH Aachen University

Abstract:
Cooperative networks rely on user cooperation at the network layer to provide services, such as packet forwarding and shared access to other network resources. However, while it enables new types of networks and services, the concept of cooperation also creates new attack possibilities. For example, wireless multi-hop networks are particularly vulnerable against flooding. Thus, reliable communication in such networks requires mechanisms that allow on-path devices, such as middle-boxes, to verify the origin and authenticity of network traffic and to stop malicious packets early in the network. This thesis proposes a set of novel cryptographic protocols for on-path authentication. The protocols are designed for flexibility and performance, allowing the approaches to scale from infrequent user authentication to continuous per-packet authentication for high bandwidth communication.