Caraoke: An E-Toll Transponder Network for Smart Cities – Public Review

Lin Zhong
Department of Electrical & Computer Engineering, Rice University, Houston, TX

E-Toll transponders are commonplace in the US: they allow vehicles to pay highway tolls electronically; and in many highways, they are actually required. The core of an E-Toll transponder is a battery-powered RFID. When queried by a radio signal from a reader, it responds by transmitting a radio signal at a fixed carrier frequency with its identity encoded. By decoding this radio signal, the reader can identify and bill the vehicle properly. However, existing transponders and readers are designed with the assumption that only one transponder responds per query. When multiple transponders responds to the same query, their responses collide because they are using the same carrier frequency and subsequently the reader will fail to decode them. Therefore today's E-Toll readers have to use directional antennas and restrict the movement of vehicles so that only one transponder responds to a query.

The authors envision a low-power, low-cost E-Toll reader that can decode simultaneous responses from multiple transponders in unrestricted vehicles, on the road or in the parking lot. They envision that a deployment of such readers along with the existing E-Toll transponders will make a city smart by knowing where the vehicles are and how fast they are moving. In this paper, they present the Caraoke reader design toward this vision, at least for outdoor line-of-sight environments. The keys to its success are two: hardware variation of transponders allows it to resolve collision in responses from multiple transponders and multiple antennas allow accurate estimates of angle of arrival. The authors demonstrated a low-power implementation of the Caraoke reader that can be potentially powered by solar energy, operating from poles of street lamps. They evaluated the counting accuracy with emulation based on data collected from 155 transponders in a campus parking lot; they evaluated the localization accuracy, speed estimation and ID decoding with a small deployment on street-lamp poles on the same campus.

The reviewers recognized this work as a *tour de force* of wireless physical layer techniques. Its novelty is in the synthesis of these techniques and applying it in building a system that promises novel applications. The reviewers were excited by its support of legacy E-Toll transponders and its low-power design, which may lower the barrier for practical adoption. The reviewers were also excited by the vision of Caraoke networks in which any vehicles with an E-Toll transponder are accounted for. The reviewers lauded the authors for providing analyses for several canonical settings and for evaluating their prototype via deployment into the streets.

The novel insight exploited by Caraoke is that hardware variation in E-Toll transponders leads to variation in the carrier frequency offset (CFO) of their responses. Although in theory all transponders should respond at the same fixed carrier frequency, in practice they do so with their own CFO. Capitalizing this variation, a Caraoke reader seeks to resolve the collision in the frequency domain and subsequently decode the responses. Hardware variation is usually considered a nuisance from imperfect manufacturing process. From mechanical parts to semiconductor circuits, people work hard to control it. However, the hardware security community has leveraged hardware variation, or more precisely *process variation*, to design physically unclonable functions. The Caraoke reader is among the first to exploit hardware variation in network system design, i.e., to exploit resulting random access in the frequency domain by E-Toll transponders. Notably, another paper at this year's SIGCOMM also exploits hardware variation to resolve collisions in responses by backscattering RFID tags. That work, however, exploits the variation in the timing, instead of CFO, of responses, and the resulting random access in the time domain.

The vision of the authors, however, asks for a more solid empirical foundation, especially for the key insight about CFO variation in E-Toll transponders. For this paper, the authors collected data from 155 transponders but could only share with readers the mean and deviation of their CFO due to privacy concern. Because the performance of Caraoke depends on the CFO distribution, practitioners interested in Caraoke are likely to examine the CFO distribution of many more transponders and how it is changing. While the authors rightly limited their design to low-cost, low-power readers, the success of their work also invites the question: what can one do with more expensive readers? For example, a reader with more antennas and more computational power can use open-loop beamsweeping to achieve better scalability, precision, and perhaps less dependence on the CFO distribution of transponders.