Editorial for TODAES Special Issue on Internet of Things System Performance, Reliability, and Security

As more low-power and Internet-connected gadgets and sensors are integrated into our lives, there are issues remaining on optimal system design of these systems. In particular, performance, reliability, and security are key parameters. Furthermore, with emerging research areas such as autonomous cars, advanced manufacturing, and smart cities and buildings, usage of Internet of Things (IoT) devices is expected to exponentially grow. This special issue focuses on the design, optimization, and security aspects of the IoT. We believe these areas are likely the key enablers for the advancements in the IoT arena.

Our special issue attracted 11 submissions. After a three-stage review process, eight papers were accepted into the special issue. We organized the special issue into three sections: (1) secure hardware, (2) system performance, and (3) system communication.

In the secure hardware section of the special issue, Yang et al. target smart manufacturing with a chipless radio-frequency identification tag that only includes features to enable resonance. These circuits are smaller in size and environmentally more friendly as compared to ones with active components in them. Hussain et al. introduce an unintelligible Hamming-distance-based authentication for physically unclonable functions (PUFs) so that the same challenge-response pairs can be used without exposure. This is an improvement to existing PUFs where responses are exposed for previously used challenges and constitute a security risk. Winograd et al. target design reverse-engineering issues by introducing a spin transfer torque magnetic reconfigurable lookup table logic. Some CMOS gates are replaced by these logic gates so that design cannot be reverse-engineered in feasible time.

For the system performance section, Truong et al. investigate recommender systems for IoT. In their implementation, expert nodes may be present or not for various recommendation rounds, but weights are used to ensure available and accurate experts are utilized often. Chopra et al. optimize data processing that should be conducted at each node of an IoT network.

In the system communication system, Hussain and Koushanfar introduce a system where a broken GPS in a car can be compensated by nearby cars to estimate the position of a car. Muztoba et al. provide an indoor navigation system that minimizes user inputs and energy spent in communication. Karabacak et al. discuss a spectral analysis-based unauthorized activity detection system based on differentiation with respect to a known test mode.

As can be observed, our special issue brings several interesting aspects of IoT system design with a variety of applications into consideration. We cover a number of cutting-edge results in secure hardware, system performance, and system communication herein. There remains much more to explore in this developing field, and we hope that readers will enjoy the special issue.

Rasit O. Topaloglu (IBM) and Farinaz Koushanfar (UC San Diego)
Guest Editors

1084-4309/2018/12-ART74e
https://doi.org/10.1145/3276908