Cyber Attacks on Internet of Things Sensor Systems for Inference

Rick S. Blum
IEEE Fellow, IEEE Signal Processing Society Distinguish Lecturer,
Robert W. Wieseman Endowed Professor of Electrical Engineering
Electrical and Computer Engineering Dept., Lehigh University

The Internet of Things (IoT) improves pervasive sensing and control capabilities via the aid of modern digitial communication, signal processing and massive deployment of sensors. The employment of low-cost and spatially distributed IoT sensor nodes with limited hardware and battery power, along with the low required latency to avoid unstable control loops, presents severe security challenges. Attackers can modify the data entering or communicated from the IoT sensors which can have serious impact on any algorithm using this data for inference. In this talk we describe how to provide tight bounds (with sufficient data) on the performance of the best algorithms trying to estimate a parameter from the attacked data and communications under any assumed statistical model describing how the sensor data depends on the parameter before attack. The results hold regardless of the estimation algorithm adopted which could employ deep learning, machine learning, statistical signal processing or any other approach. Example algorithms that achieve performance close to these bounds are illustrated. Attacks that make the attacked data useless for reducing these bounds are also described. These attacks provide a guaranteed attack performance in terms of the bounds regardless of the algorithms the estimation system employs. References are supplied which provide various extensions to all the specific results presented and a brief discussion of applications to IEEE 1588 for clock synchronization is provided.

Rick S. Blum received a B.S.E.E from Penn State in 1984 and an M.S./Ph.D in EE from the University of Pennsylvania in 1987/1991. From 1984 to 1991 he was with GE Aerospace. Since 1991, he has been at Lehigh University. His research interests include signal processing for smart grid, communications, sensor networking, radar and sensor processing. He was an AE for IEEE Trans. on Signal Processing and for IEEE Communications Letters. He has edited special issues for IEEE Trans. on Signal Processing, IEEE Journal of Selected Topics in Signal Processing and IEEE Journal on Selected Areas in Communications. He was a member of the SAM Technical Committee (TC) of the IEEE Signal Processing Society. He was a member of the Signal Processing for Communications TC of the IEEE Signal Processing Society and is a member of the Communications Theory TC of the IEEE Communication Society. He was on the awards Committee of the IEEE Communication Society. Dr. Blum is a Fellow of the IEEE, an IEEE Signal Processing Society Distinguished Lecturer (twice), an IEEE Third Millennium Medal winner, a member of Eta Kappa Nu and Sigma Xi, and holds several patents. He was awarded an ONR Young Investigator Award and an NSF Research Initiation Award.