2025 ICCST

International Carnahan Conference on Security Technology

KEYNOTE SPEAKERS

October 14-17 · San Antonio, Texas

Author Name: Rick S. Blum

Author Biography: Rick S. Blum received a B.S. in Electrical Engineering from the Pennsylvania State University in 1984 and his M.S. and Ph.D in Electrical Engineering from the University of Pennsylvania in 1987 and 1991.

From 1984 to 1991 he was a member of technical staff at General Electric Aerospace in Valley Forge, Pennsylvania and he graduated from GE`s Advanced Course in Engineering. Since 1991, he has been with the Electrical and Computer Engineering Department at Lehigh University in Bethlehem, Pennsylvania where he is currently a Professor and holds the Robert W. Wieseman Endowed Professorship in Electrical Engineering. His research interests include machine learning and signal processing for security, smart grid, communications, sensor networking, radar, and sensor processing. He was on the editorial board for the Journal of Advances in Information Fusion of the International Society of Information Fusion. He was an associate editor for IEEE Transactions on Signal Processing and for IEEE Communications Letters. He has edited special issues for IEEE Transactions 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 was 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 and served two terms as an IEEE Signal Processing Society Distinguished Lecturer. He is currently an IEEE AESS Distinguished Lecturer. He is an IEEE Third Millennium Medal winner, Eleanor and Joseph F. Libsch Research Award winner, a member of Eta Kappa Nu, a member of Sigma Xi, and holds several patents. He was awarded an ONR Young Investigator Award in 1997. His IEEE Fellow Citation ``for scientific contributions to detection, data fusion and signal processing with multiple sensors'' acknowledges contributions to the field of sensor networking.

Cyber Security of Sensor Systems for State Sequence Estimation: An AI Approach

Abstract: Due to possible devastating consequences, counteracting sensor data attacks is an extremely important topic, which has not seen sufficient study. This presentation presents the first methods that accurately identify/eliminate only the problematic attacked sensor data presented to a sequence estimation/regression algorithm under a powerful attack model. The approach does not assume a known form for the statistical model of the sensor data, allowing data-driven and machine learning sequence estimation/regression algorithms to be protected. A simple protection approach for attackers not endowed with knowledge of the details of our protection approach is first developed, followed by additional processing for attacks based on protection system knowledge. Experimental results show that the simple approach achieves performance indistinguishable from that for an approach which knows which sensors are attacked. For cases where the attacker has knowledge of the protection approach, experimental results indicate the additional processing can be configured so that the worst-case degradation under the additional processing and a large number of sensors attacked can be made significantly smaller than the worst-case degradation of the simple approach, and close to an approach which knows which sensors are attacked, with just a slight degradation under no attacks. Mathematical descriptions of the worst-case attacks are used to demonstrate the additional processing will provide similar advantages for cases for which we do not have numerical results. All the data-driven processing used in our approaches employs only unattacked training data.