Michael Hempel

University of Nebraska – Lincoln, Advanced Telecommunications Engineering Laboratory
Phone: (402) 554-3521; Fax: (402) 554-2289; Email: mhempel2@unl.edu

EDUCATION

- University of Nebraska – Lincoln, Lincoln, NE
  - Doctor of Philosophy, Computer Engineering 2007
- University of Nebraska – Lincoln, Lincoln, NE
  - Master of Engineering, Telecommunications Engineering 2002
- DTAG University of Applied Sciences, Leipzig, Germany
  - Diplomingenieur (FH) – Bachelor, Telecommunications Engineering 2000

PROFESSIONAL EXPERIENCE

- Associate Research Professor, Advanced Telecommunications Engineering Laboratory (TEL), University of Nebraska – Lincoln, July 2024- present
- Associate Director, Advanced Telecommunications Engineering Laboratory (TEL), University of Nebraska – Lincoln, August 2012-present
- Research Assistant Professor, Advanced Telecommunications Engineering Laboratory (TEL), University of Nebraska – Lincoln, September 2008- July 2024
- Postdoctoral Researcher, Advanced Telecommunications Engineering Laboratory (TEL), University of Nebraska – Lincoln, September 2007-August 2008
- Graduate Research Assistant, Advanced Telecommunications Engineering Laboratory (TEL), University of Nebraska – Lincoln, August 2000-August 2007

MEMBERSHIP IN PROFESSIONAL ORGANIZATIONS

1.	Institute of Electrical and Electronics Engineers:	Senior Member,	since 2024
		Member,	since 2007
2.	IEEE Communications Society:	Member,	since 2007
3.	National Strategic Research Institute:	Fellow,	since 2022

RESEARCH ACCOMPLISHMENTS

- Research Areas:
  - Mobile Wireless Communications
  - Cybersecurity for Operational Technology
  - Communications Protocol Design and Evaluation
  - Machine Learning and Natural Language Processing for Cybersecurity Applications
- Awarded, as Co-PI or PI, over $10 million in research grants from funding agencies such as US Federal Railroad Administration, US Department of Energy, US Department of Defense, US National Science Foundation, and more
- Author or Co-Author of over 180 peer reviewed scientific journal and conference publications

SYNERGISTIC ACTIVITIES

- Associate Editor, John Wiley's "Security and Communication Networks" journal, 2011-2017
- Technical Program Committee (TPC) member or co-chair for numerous international conferences such as IEEE ICC (2014-present), IEEE Globecom (2013-present), IEEE PIMRC (2010-present), IEEE WCNC (2010-2020), MILCOM (2011-present), or International Conference on Signal Processing and Communication Systems (2011-present)
- Reviewer for numerous journals and conferences
- Vice-Chair IEEE Computer Society, Nebraska section, 2010-2011

- Served on UNL’s Academic Standards Committee
- Currently serving on UNL’s Information Technologies and Services Committee

SELECT PUBLICATIONS

1. K. Ameri, M. Hempel, H. Sharif, J. Lopez, and K. Perumalla, “Design of a Novel Information System for Semi-automated Management of Cybersecurity in Industrial Control Systems,” ACM Transactions on Management Information Systems, vol. 14, no. 1, pp. 1–35, Jan. 2023, doi: 10.1145/3546580.

2. P. Ghasemzadeh, M. Hempel, H. Wang, and H. Sharif, “GGCNN: An Efficiency-Maximizing Gated Graph Convolutional Neural Network Architecture for Automatic Modulation Identification,” IEEE Transactions on Wireless Communications, 2023, doi: 10.1109/TWC.2023.3239311.

3. K. Ameri, M. Hempel, H. Sharif, J. L. Jr, and K. Perumalla, “An Accuracy-Maximization Approach for Claims Classifiers in Document Content Analytics for Cybersecurity,” Journal of Cybersecurity and Privacy, vol. 2, no. 2, pp. 418–443, Jun. 2022, doi: 10.3390/jcp2020022.

4. P. Ghasemzadeh, M. Hempel, and H. Sharif, “GS-QRNN: A High-Efficiency Automatic Modulation Classifier for Cognitive Radio IoT,” IEEE Internet of Things Journal, vol. 9, no. 12, 2022, doi: 10.1109/JIOT.2022.3141032.

5. P. Ghasemzadeh, M. Hempel, H. Sharif, and T. Omar, “Modeling and Performance Evaluation of an RF Transceiver System at 160 MHz for Railroad Environments,” in Proceedings of 2022 Joint Rail Conference, JRC 2022, 2022. doi: 10.1115/JRC2022-79579.

6. P. Ghasemzadeh, M. Hempel, S. Banerjee, and H. Sharif, “A Spatial-Diversity MIMO Dataset for RF Signal Processing Research,” IEEE Transactions on Instrumentation and Measurement, vol. 70, 2021, doi: 10.1109/TIM.2021.3073441.

7. S. Banerjee, P. Ghasemzadeh, M. Hempel, and H. Sharif, “Topography Relaxation in Determining Unsafe State Intersections for Uncertain CPS,” IEEE Sensors Letters, vol. 4, no. 4, 2020, doi: 10.1109/LSENS.2020.2981936.

8. S. Banerjee, M. Hempel, P. Ghasemzadeh, H. Sharif, and T. Omar, “Wireless communication for high-speed passenger rail services: A study on the design and evaluation of a unified architecture,” in 2020 Joint Rail Conference, JRC 2020, 2020. doi: 10.1115/JRC2020-8068.

9. J. Santos, M. Hempel, and H. Sharif, “Compression Distortion-Rate Analysis of Biomedical Signals in Machine Learning Tasks in Biomedical Wireless Sensor Network Applications,” in 2020 International Wireless Communications and Mobile Computing, IWCMC 2020, 2020. doi: 10.1109/IWCMC48107.2020.9148572.

SELECT RESEARCH GRANTS

1. **“CYVET: A Cyber-Physical Security Assurance Framework based on a Semi-Supervised Vetting Approach”**, Co-PI, Sponsor: Oak Ridge National Lab (Prime: Dept of Energy), 01/2020-03/2023, $844,529:

   The proposed CYVET system directly addresses the need to elevate the current industry capabilities to verify and validate OT cybersecurity and associated control system infrastructure. Currently, there is a significant gap in the energy sector's capability in that regard during infrastructure improvement, equipment procurement, and compliance certification. CYVET provides that needed capability. CYVET is device and architecture agnostic and thus broadly applicable across the energy sector. The goal of this project is to develop and deliver a cybersecurity verification and validation framework testing capability to verify and validate OT equipment, software and the underlying control system architecture. It is a machine learning-driven framework that automates the entire vetting process through substantial usage of Natural Language Processing. CYVET also incorporates a highly versatile and fully scriptable automated device testing framework that facilitates the feature claim validation and vulnerability detection, for an end-to-end processing framework uniquely applicable to OT device cybersecurity vetting.

2. **"Wireless Digital Train Line for Passenger Trains: Exploring Railroad Requirements, Achieving Synergy, and Designing WiDTL for Next-Generation Passenger Rail Services"**, Co-PI, Sponsor: Federal Railroad Administration, 08/2015-12/2023, $801,023:

   This project, currently spanning 4 phases, aims to systematically export wireless technology approaches for use in high-speed passenger trains, from control systems to passenger-centric services. With this project we have the opportunity to systematically rethink all facets of train communication. Phases 1 and 2 focused on train control communications, developing new paradigms for trainline communication, exploring principles such as data/control plane separation, as well as investigating different approaches to wayside communication. Phase 3 focused on developing a new methodology for enriching RF spectrum resources by modernizing the use of underutilized legacy RF bands already owned by the North American rail industry, and the current Phase 4 expands that effort to incorporate cognitive radio technology approaches in the pursuit of a highly modular, universal, wireless communication architecture for rail services.

3. **"Industrial Control System Cyber-Security Monitoring Solution"**, Co-PI, Sponsor: National Strategic Research Institute (Prime: Dept of Defense, USSTRATCOM), 12/2016-01/2018, $148,029:

   Developing and maintaining capabilities for the Nation requires long-term commitment. U.S. Strategic Command (USSTRATCOM) exercises operational command and control of the world's premier strategic space, cyberspace, and nuclear forces. Skilled adversaries may attempt to offset these advantages through cyber-attacks against the Industrial Control Systems (ICS) of the new USSTRATCOM Command and Control Facility (C2F) in order to create a momentary strategic advantage. This project aims to identify the best unified cyber-security solution(s) for defending the C2F ICS.

   There are three main objectives for this project. First, research and identify threats and vulnerabilities in the C2F ICS architecture that a well-resourced adversary would exploit in order to disrupt USSTRATCOM's command operations, telecommunications, and information technology systems. Second, identify, compare, and evaluate commercial and government hardware/software cybersecurity solutions capable of mitigating the identified risks. Finally, compile specific technical, operational, and maintenance data on ICS components.

4. **"Research & Development - Development of a Standard Communication Protocol for Wireless Sensor Networks in Mobile Railroad Environments"**, Co-PI, Sponsor: Federal Railroad Administration, 07/2010-07/2015:

   North America's railroad industry is envisioning a future where all aspects of freight trains can be monitored in realtime, all-the-time, whether the train is in a yard or moving across the country. However, current Wireless Sensor Network protocols are infeasible to be employed onboard freight trains. After discussions with the freight rail industry and its stakeholders, and performing a preliminary study of the major problems associated with current WSNs, this project aimed to develop a set of new approaches for standards-based WSN technologies that overcome these issues and enable robust and reliable freight train WSNs.