Brian Kim

✉brian.kim628@gmail.com http://bkim628.com ☎+1(240) 302-5616

NATIONALITY

United States and **Republic of Korea** (Dual citizenship)

CURRENT APPOINTMENT

DEVCOM U.S Army Research Laboratory, MD, USA
Postdoctoral research associate, September 2023 to present

EDUCATION

Northeastern University, Boston, MA, USA
Postdoctoral research associate, September 2022 to September 2023
Advisor: Prof. Kaushik Chowdhury (Now **University of Texas at Austin**)
University of Maryland, College Park, MD, USA
Ph.D., Electrical Engineering, September 2017 to September 2022
Advisor: Prof. Sennur Ulukus
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea
Master of Science, Electrical Engineering, March 2014 to February 2016
Advisor: Prof. Joonhyuk Kang
Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Republic of Korea
Bachelor of Science, Electrical Engineering, March 2008 to February 2014

RESEARCH INTERESTS

Wireless communications, machine learning, adversarial machine learning, covert communications, Open-RAN, Reinforcement learning, Heterogeneous Networks Routing

PROFESSIONAL EXPERIENCE

Intelligent Automation, Inc (now BlueHalo)
June 2019 to April 2022 Maryland, USA
Part Time Research Scientist

LG display R&D center
January 2015 to Febuary 2015 Paju, Republic of Korea
Intern

Electronics and Telecommunications Reasearch Institute (ETRI)
June 2010 to August 2010 Daejeon, Republic of Korea
Intern

TEACHING EXPERIENCE

Graduate Teaching Assistant University of Maryland
September 2017 to May 2019 College Park, MD, USA
Elements of Discrete Signal Analysis (ENEE 222) in Fall 2017 & Fall 2018,
Signal and System Theory (ENEE 322) in Spring 2018
Engineering Probability (ENEE 324) in Spring 2019.

PUBLICATIONS

Journal Papers

1. **B. Kim,** Y. Sagduyu, K. Davaslioglu, T. Erpek and S. Ulukus, *Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers,* IEEE Transactions on Wireless Communications, 2021.
2. **B. Kim,** Y. Sagduyu, and S. Ulukus, *Adversarial Machine Learning for NextG Covert Communications Using Multiple Antennas,* Entropy, 2022.

Conference Papers

1. **B. Kim**, J. Kong, T. J. Moore and F. T. Dagefu, *Reinforcement Learning for Covert Heterogeneous Wireless Network Routing with a Threat Region,* IEEE Consumer Communications & Networking Conference, January 2025.
2. **B. Kim**, J. Kong, T. J. Moore and F. T. Dagefu, *Reinforcement Learning Based Covert Routing with Node Failure Resiliency for Heterogeneous Networks,* IEEE Military Communications Conference, October 2024.
3. C. Tassie, **B. Kim**, J. Groen, M. Belgiovine and K. R. Chowdhury, *Leveraging Explainable AI for Reducing Queries of Performance Indicators in Open RAN,* IEEE International Conference on Communications (ICC), June 2024.
4. J. Groen, M. Belgiovine, U. Utku, **B. Kim**, and K. R. Chowdhury, *TRACTOR: Traffic Analysis and Classification Tool for Open RAN,* IEEE International Conference on Communications (ICC), June 2024.
5. A. Z. Chiejina, **B. Kim**, K. R. Chowdhury, and V. Shah, *System-level Analysis of Adversarial Attacks and Defenses on Intelligence in O-RAN based Cellular Networks,* ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), May. 2024.
6. N. Sapavath*, **B. Kim*,** K. Chowdhury, and V. Shah, *Experimental Study of Adversarial Attacks on ML-based xApps in O-RAN,* IEEE Global Communications Conference, December 2023. (* denotes equal contribution)
7. J. Groen, **B. Kim,** and K. R. Chowdhury, *The Cost of Securing O-RAN,* IEEE International Conference on Communications (ICC), May 2023.
8. **B. Kim,** T. Erpek, Y. E. Sagduyu, and S. Ulukus, *Covert Communications via Adversarial Machine Learning and Reconfigurable Intelligent Surfaces,* IEEE Wireless Communications and Networking Conference, Austin, TX, April 2022.
9. **B. Kim,** Y. Shi, Y. E. Sagduyu, T. Erpek, and S. Ulukus, *Adversarial Attacks against Deep Learning Based Power Control in Wireless Communications,* IEEE Global Communications Conference, Madrid, Spain, December 2021.
10. **B. Kim,** Y. E. Sagduyu, T. Erpek, and S. Ulukus, *Adversarial Attacks on Deep Learning Based mmWave Beam Prediction in 5G and Beyond,* IEEE Statistical Signal Processing Workshop, Rio de Janeiro, Brazil, July 2021.
11. **B. Kim,** Y. E. Sagduyu, T. Erpek, K. Davaslioglu, and S. Ulukus, *Channel Effects on Surrogate Models of Adversarial Attacks against Wireless Signal Classifiers*, IEEE International Conference on Communications, Montreal, Canada, June 2021.
12. **B. Kim,** Y. E. Sagduyu, T. Erpek, K. Davaslioglu, and S. Ulukus, *Adversarial Attacks with Multiple Antennas Against Deep Learning-Based Modulation Classifiers*, IEEE Global Communications Conference, Taipei, Taiwan, December 2020.
13. **B. Kim,** Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, *How to Make 5G Communications "Invisible": Adversarial Machine Learning for Wireless Privacys*, 54th Asilomar Conference on Signals, Systems and Computers, Pacific Grove, CA, November 2020.
14. **B. Kim,** Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, *Over-the-Air Adversarial Attacks on Deep Learning Based Modulation Classifier over Wireless Channels*, Conference on Information Sciences and Systems, Princeton, NJ, March 2020.
15. **H. Kim,** J. Kang, S. Jeong, K. Lee, and J. Kang, *Secure Beamforming and Self-Energy Recycling with Full-Duplex Wireless-Powered Relay*, 13th Annual IEEE Consumer Communications and Networking Conference (CCNC), Jan. 2016

SKILLS

Computer Skills: MATLAB, LaTeX, C, Python
Language Skills: Korean (Native), English

COURSEWORK

Machine Learning, Advanced Numerical Optimization, Convex Optimization, Multi-user Communications, Digital Communications, Information Theory, Estimation and Detection, Random Processes in Communication and Control, System Theory

SERVICE

Technical Reviewer (journals):

- IEEE Journal on Selected Areas in Communications (JSAC) Series on Machine Learning for Communications and Networks
- IEEE JSAC Special Issue on Private Information Retrieval, Private Coded Computing over Distributed Servers, and Privacy in Distributed Learning
- IEEE Transactions on Communications
- IEEE Communications Letters
- IEEE Transactions on Mobile Computing
- IEEE Transactions on Wireless Communications
- IEEE Transactions on Vehicular Technology
- IEEE Transactions on Cognitive Communications and Networking
- IEEE Wireless Communications Magazine
- IEEE Transactions on Machine Learning in Communications and Networking

Technical Reviewer (conferences):

- IEEE International Conference on Communications (ICC)
- IEEE International Conference on Computer Communications (INFOCOM)
- IEEE Military Communications Conference (MILCOM)

Last updated: November 2024