Securely Operating Through 5G Infrastructure

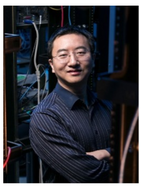
Webinar Registration Link
https://forms.gle/yX7MCSx9CJa8ZiaAA

Webinar Zoom Link: https://udc-edu.zoom.us/j/85141340870?pwd=T25zck1QclRzUE1iczJwdEI0UnQrQT09
Passcode: 1234

Date and Time
Wednesday, April 26th, 10am - 12pm

Title: Securely Operating Through 5G Infrastructure – Overview of NSF Convergence Accelerator Track G Program

Abstract: George Mason University (GMU) is the lead institution of one of the 16 teams selected by the U.S. National Science Foundation (NSF) for the Convergence Accelerator program 2022 cohort for the research topic — Track G: Securely Operating Through 5G Infrastructure. It aims at accelerating 5G solutions to assist the U.S. government and critical infrastructure operators to communicate securely anywhere and anytime. Partnering with AT&T and Michigan State University, the GMU team is developing a product, "WindTexter", that can expand the end user's capability of securely communicating over non-cooperative 5G networks by building a covert and end-to-end secure channel over indigenous 5G messaging and voice services. The multidisciplinary team is comprised of researchers, inventors, and engineers with diverse backgrounds and expertise in cybersecurity, wireless communication, artificial intelligence (AI), natural language processing (NLP), and steganography. The team is also working with the University of the District of Columbia and Morgan State University to broaden the participation for underrepresented groups. For more information about windTexter, please visit https://wirelesscyber.cec.gmu.edu/WindTexter.



Bio: Dr. Kai Zeng is currently an associate professor in the Department of Electrical and Computer Engineering at George Mason University (GMU). He is the director of the Wireless Cyber Center and Wireless Innovation and Cybersecurity Lab at GMU. He earned his Ph.D. degree in electrical and computer engineering at Worcester Polytechnic Institute (WPI), and both a M.S. in communication and information systems and a B.S. in communication engineering from Huazhong University of Science and Technology, China. Dr. Zeng received an NSF CAREER award in 2012, the Excellence in Postdoctoral Research award from the University of California, Davis in 2011, and the Sigma Xi Outstanding Ph.D. Dissertation award at Worcester Polytechnic Institute in 2008. He was a visiting faculty member at the Air Force Research Lab in 2013. He has broad interests in cyber security and wireless networking with emphasis on physical layer security, cyber physical systems/IoT security, spectrum sharing, and machine learning applications. His research has been supported by NSF, DARPA, ARO, ONR, NSA, MITRE, and Commonwealth Cyber Initiative (CCI). He has served as associate editor for IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cognitive Communications and Networking, IEEE Transactions on Wireless Communications, and IEEE Transactions on Machine Learning in Communications and Networking.

Title: How We Went From 1G to 5G and Applications for AI (WindTexter)

Abstract: I will go over the history of mobility and how in the 1980's it nearly never happened and the reasons behind that.

Bio: Irwin Gerszberg AT&T Fellow and Distinguished Inventive Scientist for AT&T Labs in Middletown, NJ. He is responsible for Advanced RF Research technologies on Department of Defense 5G mobility projects, emerging broadband infrastructure such as Project AirGig™, and heads up the AT&T Science and Technology Innovation Center. He holds a bachelor's degree and a master's in Computer Science from the New Jersey Institute of Technology and Stevens Institute of Technology. He joined the AT&T Bell System in 1978 where he spearheaded AT&T's first speech response/voice recognition system. After joining AT&T's Wireless unit, he was responsible for the development of numerous advanced wireless technologies and services. Over the years Irwin has made key fundamental contributions to Science and Technology in Digital Subscriber Line, voice over DSL, IP based cable telephony, broadband wireless, broadband over powerline, microcells, satellite, fixed wireless, high definition Voice, IP telephony, and a vast array of emerging broadband infrastructure initiatives. He holds an amazing record, 675+ patents with the United States Patent Office on advanced technologies covering a vast array of wireless, wired, and emerging broadband technologies. In 2001 he received AT&T's Science and Technology medal. In 2002, he was inducted into the New Jersey Inventors Hall of Fame by the Governor of the State of New Jersey for his innovations and contributions to science and technology in the telecommunications industry. In 2004, he was awarded AT&T's highest honor: The AT&T Fellow Award for his long-term career in pioneering contributions and innovations for the telecommunications industry. Today within AT&T, Irwin Gerszberg is simply known as the father of Project AirGig™ which is a technology that enables Gigabit data tansmission on Electric utility power lines.

Title: Multi-path over 5G for Security and Resilience Enhancement

Abstract: Multi-path transmission exploits the availability of multiple paths through a network, usually with the objective of increasing overall data rates and reducing latency. In this talk, we explore the idea of using multi-path transmission to enhance the security and resilience of communicating over potentially non-cooperative or even hostile 5G networks. Data transmission over multiple paths, in conjunction with encryption and erasure codes, can provide greater protection against adversarial threats such as eavesdropping and jamming. As we shall discuss, multi-path over 5G presents some interesting tradeoffs among performance, security and resilience. Joint work with Massieh Kordi Boroujeny, Huacheng Zeng, and Kai Zeng.

Bio: Brian L. Mark is a professor in the Dept. of Electrical and Computer Engineering at George Mason University. He received the Ph.D. in electrical engineering from Princeton University and a B.A.Sc. degree in computer engineering from the University of Waterloo. Prior to joining George Mason University in 2000, he was a Research Staff Member at NEC Laboratories America in Princeton, New Jersey from 1995-1999. His research interests are broadly in the areas of communications, computer networks, and signal processing with a focus on wireless networks, performance modeling, and network security.

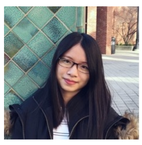
Title: Location Privacy Risk of 5G Smart Devices

Abstract: Smart devices such as AirPods and smartwatches have become commonplace in our daily lives, connecting to our smartphones through Bluetooth for more convenient user interaction and internet access. However, the frequent transmission of Bluetooth radio signals between these devices (often hundreds of data packets per second) can pose a serious privacy risk. Specifically, this type of Bluetooth signal transmission on a person's body (e.g. on their wrist or in their ear) can enable malicious actors to estimate the user's location with high accuracy in real time. In this presentation, I will discuss the potential design of a radio eavesdropper capable of estimating the location of Bluetooth devices in real time, even through walls. Furthermore, I will demonstrate the implementation of this technology in practice. To address this privacy risk, I will also suggest possible countermeasures that can be used to protect individuals' location privacy if needed.

Bio: Huacheng Zeng is an Assistant Professor in the Department of Computer Science and Engineering at Michigan State University. He is a recipient of NSF CAREER Award. His research interest is broadly in wireless networking and sensing systems.

Title: Hiding Text in Text with Generative AI

Abstract: In this presentation, I will give a brief overview to linguistic steganography, i.e., hiding information in natural language texts for covert and secure communication. Traditional linguistic steganography systems are mostly edit-based, e.g., encoding information via substituting synonyms in a cover text, which often leads to limited capacity and unnatural stego texts. The emergence of large language models (e.g., OpenAI GPTs) in recent years revealed a promise of generation-based linguistic steganography, where a natural stego text can be directly generated from a pre-trained language model. This talk will introduce and compare both types of approaches, hoping to offer insights to the community.



Bio: Ziyu Yao is an Assistant Professor in the Department of Computer Science at George Mason University, where she co-leads the George Mason Natural Language Processing (NLP) group. Her research has been focusing on building natural language interfaces that can reliably assist humans in knowledge acquisition and task completion, including their applications to other disciplines (e.g., software engineering, IO psychology, healthcare). More about her can be found at https://ziyuyao.org/.

Title: Assessing the Socio-economic Impacts of Secure Texting and Anti-Jamming Technologies in Non-Cooperative Networks

Abstract: Operating securely over 5G (and legacy) infrastructure is a challenge. In non-cooperative networks, malicious actors may try to decipher, block encrypted messages, or specifically jam wireless radio systems. Such activities can disrupt operations, from causing minor inconvenience, through to fully paralyzing the functionality of critical infrastructure. While technological mitigation measures do exist, there are very few methods capable of assessing the socio-economic impacts from different mitigation strategies. This leads to a lack of robust evidence to inform cost-benefit analysis, and thus support decision makers in industry and government. Consequently, this paper presents two open-source simulation models for assessing the socio-economic impacts of operating in untrusted non-cooperative networks. The first focuses on using multiple non-cooperative networks to transmit a message. The second model simulates a case where a message is converted into alternative plain language to avoid detection, separated into different portions and then transmitted over multiple non-cooperative networks. A probabilistic simulation of the two models is performed for a 15 km × 15 km spatial grid with 5 untrusted non-cooperative networks and intercepting agents. The results are used to estimate economic losses for private, commercial, government and military sectors. The highest probabilistic total losses for military applications include US$300 ± 25, US$150 ± 15, and US$75 ± 10, incurred for a 1, 3 and 5 site multi-transmission approach, respectively, for non-cooperative networks when considering 1,000 texts being sent. These results form a framework for deterministic socioeconomic impact analysis of using non-cooperative networks and secure texting as protection against radio network attacks. The simulation data and the open-source codebase is provided for reproducibility.

Bio: Dr. Edward J. Oughton has been working on critical infrastructure modeling and simulation for over ten years, having been awarded over $1 million in research funds in this area. His PhD and post-doctoral research were funded by the UK's Engineering and Physical Sciences Research Council where he developed decision support models for broadband infrastructure, with a strong focus on wireless communications such as 5G. This included carrying out assessments of 5G strategies for the UK Treasury, Dutch Ministry of Economic Affairs, and over 20 other governments around the world. Recently, he built the International Monetary Fund's Digital Infrastructure Cost Estimator to help quantify universal broadband investment needs, with the tool being applied to 190 countries globally. The critical infrastructure modeling techniques he has developed have also been used for risk analysis. This has included carrying out quantitative assessment of cyber-attacks on London's electricity distribution network (awarded Runner-Up in the Lloyd's of London Science of Risk Prize), as well carrying out assessments of space weather risks to electricity transmission infrastructure in the USA and UK (winning Best Paper 2019 in the journal Risk Analysis). In 2017, Dr Oughton was selected by the US Embassy (London) to take part in the US International Visitors Leadership Program on the cyber-security of critical infrastructure. He retains honorary positions at the University of Oxford Environmental Change Institute, and with the British Antarctic Survey Space Weather and Atmosphere Group. He holds an MPhil and PhD in urban and regional economics from the University of Cambridge. He has published over thirty peer-reviewed publications on research pertaining to critical infrastructure.

Event Organizer

Bio: Dr. Amir Alipour-Fanid is an assistant professor in the Department of Computer Science and Information Technology at University of the District of Columbia (UDC). He received his Ph.D. degree in Electrical and Computer Engineering at George Mason University in 2021. Prior to joining UDC, he was a senior researcher with the Architectures and Security team at General Motors (GM). His research interests are in the intersection of cybersecurity and machine learning, and he is doing research in the area of cyber-physical systems (CPS) security, 5G communication security, Internet-of-Things (IoT) security, connected and autonomous vehicles security, theoretical and applied machine learning. Dr. Alipour-Fanid was a recipient of the Outstanding Academic Achievement Award from George Mason University.