Research Statement

Ebuka Philip Oguchi

Rapid advancements in wireless communication technology have revolutionized how we live and interact with the world, radically changing industries like molecular communication, autonomous vehicles, and agriculture. But these advancements have also brought hitherto unprecedented cybersecurity challenges, notably about guaranteeing message integrity and authenticity in settings where traditional cryptographic techniques are insufficient. The hazards of passive and active attacks increase with our reliance on these wireless platforms, and these concerns are further compounded by the broadcast nature of the wireless medium and the quick commercialization of new products. My work at the University of Nebraska–Lincoln was focused on creating strong physical layer security techniques to address these issues. My work develops scalable, interoperable, and secure solutions by combining cutting-edge techniques from machine learning, cryptography, and signal processing to guarantee the reliability of communication networks in various specific applications. My passion for cybersecurity results from my strong desire to create robust systems that safeguard vital infrastructures and improve the security and effectiveness of new technological developments.

Past Research

My Ph.D. research concentrated on fundamental security issues at the interface of privacy, security, usability, and efficiency in wireless networks. My research focuses on cybersecurity in the agricultural, vehicular, machine learning, and molecular industries. I specialize in message integrity and authentication for commercial off-the-shelf (COTS) wireless devices, drawing on my experience in machine learning, cryptography, and security. My research findings have appeared in leading peer-reviewed conferences such as EAI SecureComm and IEEE INFOCOM, and a journal is under review in ACM Transactions on the Internet of Things. My current publications have contributed to the Nebraska Center for Energy Sciences Research (NCESR) grant and NSF-funded projects (CNS-2225161, CNS-2331191, and CNS-1619285, ECCS-2030272), demonstrating my work's significant impact and relevance in advancing wireless communication system security. Through my efforts, I hope to contribute to creating a more secure and robust digital infrastructure capable of withstanding the changing threats posed by hostile actors across multiple domains. My main contributions include:

Agricultural IoT Security: Ag-IoT proliferation has considerably improved farming practices by increasing crop yields and maximizing resource utilization. However, real-time data collected by underground sensors is extremely sensitive, and any distortion could have serious effects, such as reduced agricultural output and waste of resources. My work on the STUN (Secret-Free Trust-Establishment for Underground Wireless Networks) protocol focuses on ensuring secure data transfer between underground sensors and aboveground gateways. STUN ensures secure bootstrapping and message integrity without relying on preloaded secrets or complex cryptographic algorithms by exploiting underground wireless signal propagation characteristics that are difficult to hack. This protocol is designed to withstand aggressive signal injection attempts, making it highly scalable and suitable for

commercial off-the-shelf (COTS) devices in various farming contexts. The STUN protocol's security equivalency with the Unbalanced Oil and Vinegar (UOV) cryptosystem illustrates its resistance to advanced adversaries, guaranteeing that farming operations remain secure and resilient. The results of this work were published in IEEE INFOCOM. In addition, one manuscript is submitted to ACM Transaction on Internet of Things.

Autonomous Vehicle Security: The rise of self-driving cars, especially connected autonomous vehicles (CAVs) and unmanned aerial vehicles (UAVs), creates new security issues, particularly in determining the authenticity of position and velocity data. Traditional encryption technologies are vulnerable to attacks by adversaries equipped with strong antennas. To overcome this, I developed the VET (Autonomous Vehicular Credential Verification using Trajectory and Motion Vectors) framework. This framework uses trajectory and motion vector data to authenticate communications and prevent adversaries from injecting malicious data. VET's revolutionary technique is not based on assumptions about the wireless environment, such as the number of reflectors or the center frequency. Our experimental evaluations demonstrate that VET effectively detects and mitigates attacks, even from advanced remote adversaries, ensuring the safety and reliability of autonomous vehicle operations. This work is crucial as the adoption of autonomous systems grows, and the potential for malicious interference becomes a more pressing concern. The results of this work were published at EAI SecureComm (28.9% acceptance rate)

Radio Frequency Fingerprinting: Ensuring message integrity in underground networks is critical, especially in scenarios where typical cryptographic identities are insufficient. My current radio frequency fingerprinting study focuses on finding unique wireless physical layer properties for devices and locations using machine learning methods. This solution adds an extra degree of protection, similar to second-factor authentication, by confirming the legitimacy of messages based on their physical transmission features. This research is especially important for underground networks, where environmental conditions can dramatically affect signal propagation. The study is designed to fill significant gaps in wireless communication security in demanding circumstances where the physical features of the transmission medium can be used to improve security. A manuscript covering these contributions is currently under preparation.

Molecular Communication Security: As nanotechnology advances, secure communication between nanodevices becomes more crucial. My research in molecular communication security focuses on maintaining message integrity in biological contexts where typical electromagnetic-based communication technologies are unfeasible. I am working on lightweight security techniques to safeguard molecular channels from potential adversaries such as harmful nanodevices or bioterrorism threats. This study is critical for applications in drug delivery and nanomedicine, where secure communication is critical to the safety and efficacy of medical treatments. This study explores the interaction of chemical and biological processes with communication protocols, opening up new avenues for protecting future nanoscale technologies. A manuscript covering these contributions is currently under preparation.

Future Research Agenda

I envisage a future in which wireless communication technologies are naturally secure,

adaptive, and resilient, easily integrating into various industries, including agriculture, autonomous vehicles, healthcare, and critical infrastructure. These solutions will safeguard sensitive data and enable individuals and enterprises to use secure communication technologies regardless of technological proficiency. To accomplish this mission, I will continue to create unique security mechanisms based on cutting-edge machine learning, cryptography, and signal processing approaches. My research will focus on developing solid solutions to existing risks that are adaptive to future difficulties, ensuring that secure communication is a basic component of tomorrow's technological achievements. Building on my current work, I intend to broaden my research in the following areas:

Advanced Trust Establishment in Emerging Technologies: New security challenges emerge as wireless technologies advance, particularly with the introduction of mmWave and 5G. I'll look into advanced trust-establishing approaches designed specifically for these environments, focusing on guarding against active adversaries in MIMO systems. My research will also look at constructing and developing secure device-to-device (D2D) communication lines that do not require intermediary base stations. This is critical for enabling direct, peer-to-peer communication in 5G networks. The findings of this study offer the potential to establish new standards for secure communication in next-generation wireless networks, making them more resilient to increasingly sophisticated attacks.

Post-Compromise Security Recovery: Recognizing that device penetration is often unavoidable, I intend to create automatic recovery methods to restore network secrets following a breach. My research will focus on developing strong systems that distinguish between legitimate devices and attackers even after a full compromise. This effort is crucial to ensuring network integrity in the face of advanced persistent threats. It will help develop self-healing systems capable of quickly recovering from security issues.

Non-Cryptographic Secret Evolution: Traditional cryptographic approaches, while effective, may not be sufficient in highly dynamic or limited contexts. I will investigate non-cryptographic, context-independent key evolution strategies for improving wireless network security. This includes investigating new ways to derive secrets from ambient occurrences and improving the entropy of such secrets. This research, which focuses on non-cryptographic techniques, has the potential to provide lightweight yet secure alternatives in environments where conventional cryptography is not feasible.

Cybersecurity for Emerging Applications: As new wireless communication applications emerge, particularly in autonomous vehicles, smart agriculture, and other IoT domains, unique security challenges arise. I plan to expand my research to solve these issues by building specific security measures to ensure these systems operate safely and securely. This effort is critical as these technologies become more integrated into daily life, and security becomes increasingly important to their adoption and success.

Interdisciplinary Collaborations and Impact:

Deploying secure network systems across numerous sectors, such as agriculture, trans-

portation, and healthcare, opens up tremendous opportunities for multidisciplinary study. I have collaborated with experts from diverse fields, such as agriculture, biological science, social networks, and computer science, to develop comprehensive security solutions. For example, my collaboration with computer scientists, agricultural experts, and engineers has led to the development of secure communication protocols for smart farming devices. My collaboration with social scientists, biological scientists, and engineers has led to exploring secure communication protocols for molecular communication. Additionally, I have engaged and interacted with transportation engineers to explore safeguarding communication channels in connected vehicle networks, where the integrity of transmitted data is crucial for safety and efficiency. I intend to work collaboratively with domain experts and industry partners to develop further comprehensive security solutions that meet the unique issues of these industries. For example, I plan to design secure communication protocols for medical equipment and sensors in the healthcare industry, guaranteeing that patient data is safeguarded from unauthorized access. Similarly, in the transportation industry, I will research safeguarding communication channels in connected vehicle networks, where the integrity of transmitted data is critical for safe and efficient operation.

Beyond these applications, I'm eager to work with machine learning, data science, and systems engineering experts to investigate how emerging technologies can improve security procedures. Collaborations in other sectors, such as critical infrastructure and industrial control systems, will allow for the development of more resilient and scalable security solutions. Working with industry partners will also be important since it enables the practical implementation of research findings and ensures that the solutions created are viable and effective in real-world contexts.

These synergistic activities have the potential to yield significant results, not only in advancing academic knowledge but also in delivering tangible benefits to society by improving the safety, security, and efficiency of critical systems across multiple domains.

Broader Impact and Global Contribution:

My research has profound implications outside academia, with the potential to address some of today's most critical global concerns. My research can help to improve global food security by making smart farming devices more resilient to cyberattacks, thereby safeguarding crop production and maximizing resource use. My research on autonomous vehicles ensures safer transportation networks, lowering the risk of accidents and saving lives. In healthcare, medical device security is crucial for improving patient outcomes, safeguarding sensitive health data, and advancing public health. By creating scalable and interoperable security protocols, I hope to impact international standards for secure communication networks, guaranteeing that my research contributes to building a globally resilient digital infrastructure.

My commitment to a wider impact includes participating in global collaborations. Working with international research teams, I aim to create solutions that address regional cybersecurity concerns while contributing to global progress. Whether through academic collaborations, corporate partnerships, or public policy initiatives, I aim to ensure that my study's findings are broadly accepted and have a long-term, positive impact on society.

Funding Application Strategy:

I plan to seek external funding from various sources to support my research agenda. My primary priority will be to submit a proposal for the NSF Faculty Early Career Development Program (CAREER), which will allow me to lay a solid foundation for my research. In addition, I want to submit proposals to numerous NSF initiatives, including the Secure and Trustworthy Cyberspace (SaTC) program and the Computer and Network Systems (CNS) division. These programs are strongly related to my research interests and offer opportunities for transdisciplinary, high-impact projects.

I will also explore funding opportunities from security-related agencies like the Defense Advanced Research Projects Agency (DARPA), the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Intelligence Advanced Research Projects Activity (IARPA), and the Office of Naval Research (ONR). These agencies provide significant funding for innovative research to improve cybersecurity across various sectors, making them perfect collaborators for my work. Furthermore, I plan to seek funding from the Department of Defense (DoD), the Army Research Organization (ARO), and the Department of Energy's (DOE) Cybersecurity for Energy Delivery Systems (CEDS) program, which prioritizes critical infrastructure protection and national security. These many funding sources will enable me to pursue cutting-edge research while ensuring my work remains aligned with national and global priorities.

Summary:

My research is motivated by a desire to build the next generation of computer and communication systems with excellent security and performance. My experience as a Teaching Assistant and Research Assistant at the University of Nebraska-Lincoln has given me great insights into the practical problems of cybersecurity education and research. This experience has influenced my approach to building security solutions that are both theoretically sound and practically usable, assuring their effectiveness in real-world scenarios.

The University of XXXXXXX provides exceptional resources that will assist me in building an active research group and securing external funding. The Department of XXXXXXX has strengths across disciplines, and potential collaboration with current faculty members, such as Dr. XXXXXXX, Dr. XXXXXX, and Dr. XXXXXX, will benefit my research in various ways. My cybersecurity expertise and research can make immediate and long-term contributions to the department's education and research programs.

Through my research, I aim to develop innovative security mechanisms that will protect critical infrastructures, enhance the safety of technological advancements, and contribute to the broader societal goal of creating a secure and resilient digital world.