NORD GRANT APPLICATION

| **Contact Information:** | |
|---|---|
| Last Name, First Name | Miri Lavasani, Seyed Hossein |
| Alphanumeric CWRU ID | sxm1243 |

**PURPOSE:** describe the rationale and scope of the project.

The Fourth Industrial Revolution (FIR) is characterized by a fusion of technologies that is blurring the lines between physical, digital and biological spheres, collectively referred to as cyber-physical systems. Smart connected multi-functional sensors are playing an important role in such systems, enabling a variety of key applications through a global connectivity network called Internet of Things (IoT). The proliferation of IoT into various aspects of human life including critical applications such as remote medicine and smart infrastructure, necessitate secure communication for the sensor modules through the network.

Secure data communication has been historically viewed by researchers as a software- and system-level challenge imposing a strict requirement on the design of the digital signal processing (DSP) blocks used in radio transceivers. However, due to the low-cost nature of multi-functional sensor systems, these systems lack sufficient processing power to perform complicated data encryption/decryption. On the other hand, hardware-level security enhancement methods, particularly those focused on the radio front end, are more power efficient and easier to implement. They will also add real-time security features to the system. This study aims to develop cost-effective low-power secure radio links for multi-functional sensor modules in 12 months. The project will enable prototype modules that do not require sophisticated encryption or complicated backend signal processing to create a cost-effective low-power secure link for IoT systems. The plan is to add the security feature to off-the-shelf radio transceivers and interface them with the multi-sensor module to create a secure sensor link. The security feature will be implemented in the radio front-end using innovative techniques such as signal phase shifting that rely on creating intentional mismatch in the design such that the received signal is either lost or unrecoverable when the radio link is compromised.

In addition to enhancing the student's knowledge and providing the critical hands-on experience to prepare the student for his/her career after the graduation, this project allows the PI to enhance the electronic circuit design course curriculum at CWRU by incorporating developed novel techniques in traditional RF/analog circuit design courses. Moreover, it will allow the PI to develop new laboratory experiments to get undergraduate and graduate students familiar with the important topic of hardware security in electronic circuits. The findings can also motivate other instructors at CWRU to include hardware security in other courses that deal with other blocks in the system, including the sensors and biomedical implants.

**STUDENT IMPACT:** how will this project improve CWRU student learning?

This project will have a significant impact on the students learning at CWRU. In addition to developing critical theoretical knowledge of hardware security for radios used in IoT applications, they will gain hands-on experience with designing a wireless sensor system. They will also learn how to incorporate key security features in their design and protect the system against intrusion while maintaining the essential functionality of the wireless sensor system in normal operating mode. This will significantly enhance students' knowledge of various security protocols as well as implementation and debugging issues in real-life scenarios, preparing them for careers in both industry and academia in modern smart IoT era. There is also an opportunity for collaboration with leading researchers in the field through my existing collaborations with faculties at the Ohio State University where a new AFOSR-supported center focusing on hardware security is inaugurated. This collaboration will go a long way to introduce students to various aspects of hardware security for other more complicated electronic systems used in high performance applications such as ultra-high speed wireline transceivers and secure antenna arrays.

NORD GRANT APPLICATION

**PROFESSIONAL IMPACT**: how will this project demonstrate innovation in teaching and research?

This project will enhance the teaching by incorporating innovative hardware security techniques in electronic circuit design courses and prepare the students to pursue careers in electronics during the era of smart IoT. It will revolutionize the curriculums in undergraduate- (e.g. EECS 344) and graduate-level (e.g. EECS 426 and EECS 600: RFIC Design) electronic courses which are currently focused on conventional analog and RF circuit design techniques developed before the concept of smart always-connected systems became popular. In addition to that, the successful completion of the project will allow for designing lab experiments that can give students a useful insight into real challenges in secure connected systems.

The impact of this research will be significant in the community too as the innovative hardware-level security techniques developed during this project can help advance the state-of-the-art in cyber-physical security by enabling real-time low-power approaches with minimal backend complexity. The developed low-power RF/analog security techniques can revolutionize the industry by creating a new family of secure embedded systems used in critical applications such as factory automation where electronic control units play a key role in the overall functionality of the smart system.

**METRICS AND DATA COLLECTION** measures of the project's success and CWRU student learning.

This project will be conducted over the course of one year. The research will be conducted by a student under the supervision of the PI. The course curriculum enhancement and designing lab experiments will be done by the PI. The project is divided into three major tasks (i.e. milestones) shown in the following table. Upon completion of each section, a lab demonstration will be performed by the student to show the successful accomplishment of the task with the last demonstration showcasing the complete secure and connected sensor module. In addition to the final report submitted to UCITE within two months of project end date, the findings from each milestone is compiled into a report by the student and delivered to the PI after the successful demonstration in the lab.

| Tasks/Deliverables | Timeline |
|---|---|
| Design and demonstration of wireless connectivity module | 05/01/2020 |
| Design and demonstration of secure wireless communication; enhancing the RF/analog circuit design course curriculum with hardware security; Designing lab experiments to incorporate security in analog electronics | 09/01/2020 |
| Integrating the security feature into the wireless sensor module and demonstrating the secure and connected sensor module | 12/31/2020 |

**UCITE FUNDS:** How the funding requirements align with UCITE's mission of innovative teaching and CWRU student learning.

Keeping student training and education program up-to-date and consistent with the expectation of employers in the job market is a pivotal task for any academic organization training students in STEM disciplines. Funding this project will go a long way in preparing the students for their career by giving them the necessary knowledge and hands-on experience on the important topic of hardware security. In addition to that, the funding will allow the PI to dedicate a portion of his time not only to supervise the student during the course of the project but also enhance the RF/analog circuit design course curriculum by exposing the students to RF/analog security techniques needed in modern radio transceivers.

Budget for Nord Grant

Name: Seyed Hossein Miri Lavasani

Title of Project: Secure and Connected Smart Sensor Modules

Department of Electrical, Computer, and Systems Engineering

Case School of Engineering

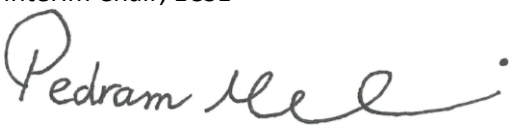
| **Expenses** | |
|---|---|
| Resource materials for the project (includes sensors, radio chips, security chips, software) | 3,000 |
| Summer Salary | 2,925 |
| Fringe Benefits for Summer Salary | 975 |
| **Total Expenses** | 6,900 |
| **Cost Sharing** | |
| Graduate Assistant (1 student, 10 hours/week @ $13/hour, for 12 months) | 6,500 |
| Books purchased with department funds | 100 |
| Travel to conference | 300 |
| **Total Cost Sharing** | 6,900 |

Seyed Hossein Miri Lavasani

Assistant Professor, ECSE

Pedram Mohseni, Ph.D.

Interim Chair, ECSE



CASE WESTERN RESERVE UNIVERSITY
CASE SCHOOL OF ENGINEERING

**Electrical, Computer, and Systems Engineering**

10900 Euclid Avenue
Glennan Building 517-B
Cleveland, Ohio 44106-7071

Phone: 216.368.5263
Fax: 216.368.6888
Email: pedram.mohseni@case.edu
URL: www.mohsenilab-cwru.org

October 28, 2019

Dear UCITE Nord Grant Committee:

It is my pleasure to support Prof. Hossein Miri Lavasani's proposal entitled "Secure and Connected Multi-Sensor Modules". Hossein is a newly hired Assistant Professor in the electrical, computer, and systems engineering (ECSE) department focusing on smart sensor interfaces for Internet-of-Things (IoT). He has a vision for creating a network of secure and smart sensors for IoT that can be used in critical infrastructure and sensitive biomedical applications.

I have had an initial review of his proposal along with his proposed budget. I believe the new student research experience, curriculum enhancement, and hands-on teaching innovations fit well with the goal of improving student learning in our ECSE department. The proposed project goes a long way to enrich students' knowledge of the critical issue of security in today's always-connected world. I also believe the project can be accomplished within the proposed 1-year timeline, and the requested budget is justified. Completing this project is an appropriate endeavor at this point in Prof. Lavasani's career as a new investigator in our department. Given the importance of hardware security in smart sensors, the ECSE department is willing to support this project by providing 1:1 matching fund from internal resources. Please do not hesitate to contact me should you need any additional information. Thank you!

Best regards,

Pedram Mohseni, Ph.D.
*Professor* and *Interim Chair*

Electrical, Computer, and Systems Engineering Dept
Biomedical Engineering Dept (Secondary)
Case Western Reserve University

**Hossein Miri Lavasani (**Email: sxm1243@case.edu)

## Education

2004-2010 **Georgia Institute of Technology,** Atlanta, Georgia
Ph.D. in Electrical and Computer Engineering (Analog/Mixed-Signal IC Design)

2001-2003 **Arizona State University,** Tempe, Arizona
M.S. in Electrical Engineering (RF/Analog and Mixed-Signal IC Design)

1997-2001 **Sharif University of Technology**, Tehran, Iran
B.S. in Electrical Engineering (Electronics)

## Appointments

2019-Present **Assistant Professor,** Case Western Reserve University, Cleveland, OH

2017-2019 **Sr. Staff RF/Analog IC Design Engineer,** Qualcomm-Atheros Inc., *San Jose, CA*

2014-2017 **Staff RF/Analog IC Design Engineer,** Qualcomm-Atheros Inc., *San Jose, CA*

2012-2014 **R&D Analog IC Design Engineer 4 (Chip Lead),** Avago Technologies Inc., *San Jose, CA*

2010-2012 **R&D Analog IC Design Engineer 3,** Avago Technologies Inc., *San Jose, CA*

## Selected Honors and Awards

2017 Best student paper award for B. Mathieu *et al.* in IEEE Compound Semiconductor IC Symposium

2017 IEEE Senior Member

2008 IEEE Electron Devices Society student grant for presentation at the IEDM 2008

## Selected Publications

- B. L. Mathieu, J. J. McCue, L. Duncan, B. Dupaix, **H. M. Lavasani**, and W. Khalil, "A Capacitively Coupled, Pseudo Return-to-Zero Input, Latched-Bias Data Receiver," *IEEE J. Solid-State Circuits* **(*Invited*)**, vol. 53, no. 9, pp. 2500-2511, Sep. 2018.
- M. Sharifzadeh, A. H. M. Shirazi, Y. Rajavi, **H. M. Lavasani**, M. Sharifzadeh, and M. Taghivand, "A Fully Integrated Multi-Mode High-Efficiency Transmitter for IoT Applications in 40nm CMOS," accepted for presentation in *IEEE Custom Integrated Circuits Conference (CICC)*, Apr. 2018.
- B. Mathieu, J. J. McCue, B. Dupaix, V. J. Patel, S. Dooley, J. Wilson, **H. M. Lavasani**, and W. Khalil, "An AC Coupled 10 Gb/s LVDS-compatible Receiver with Latched Data Biasing in 130 nm SiGe BiCMOS," in *IEEE Compound Semiconductor IC Symposium (CSICS)*, Oct. 2017 **(Best Student Paper Award)**.
- H. M. Shirazi, **H. M. Lavasani**, M. Sharifzadeh, Y. Rajavi, M. Taghivand, and S. Mirabbasi, "A 980µW 5.2dB-NF Current-Reused Fully Integrated Direct-Conversion Bluetooth-Low-Energy Receiver in 40nm CMOS," in *IEEE CICC*, May 2017.
- H. M. Shirazi, H. Rashtian, R. Molavi, T. Taris, **H. M. Lavasani**, and S. Mirabbasi, "On the Design of Combined LNA-VCO-Mixer for Low-Power and Low-Voltage CMOS Receiver Front-Ends", *Microelectronics Journal*, vol. 57, pp. 34-47, Nov. 2016.
- **H. M. Lavasani,** W. Pan, B. Harrington, R. Abdolvand, and F. Ayazi, "Electronic Temperature Compensation of Lateral Bulk Acoustic Resonator Reference Oscillators Using Enhanced Series Tuning Technique," *IEEE J. Solid-State Circuits*, vol. 47, no. 6, pp. 1381-1393, Jun. 2012.
- **H. M. Lavasani,** W. Pan, B. Harrington, R. Abdolvand, and F. Ayazi, "A 76dBΩ 1.7GHz 0.18µm CMOS Tunable Transimpedance Amplifier Using Broadband Current Pre-Amplifier for High Frequency Lateral Micromechanical Oscillators," *IEEE J. Solid-State Circuits* **(*Invited*)**, vol. 46, no. 1, pp.224-235, Jan. 2011.

## Selected Patents

- M. Shirazi Nejad, M. Taghivand, **H. M. Lavasani**, and M. Emadi, "Linear Low Noise Amplifier," US Patent # 9,887,678, Feb. 2018.
- **H. M. Lavasani**, C.-H. Wang, A. Komijani, and M. Vahid Far, "Current-driven baseband filter with reduced adjacent channel leakage ratio (ACLR)," US Patent # 9,520,846, Dec. 2016.
- **H. M. Lavasani**, "Method and apparatus for automatically adjusting the bandwidth of an electronic amplifier," US Patent # 8,836,423, Sep. 2014.