Cognitive and High Frequency Long Range Communications (HF Program)

PI: Michael Marefat, PhD

Co-PI: Tamal Bose, PhD and Loukas Lazos, PhD

Coordinator: Nancy Emptage

Graduate Assistant Mentors: Jingcheng Li, Noel Teku, and Ziqi Xu

Sponsors: National Science Foundation (NSF) and University of Arizona Graduate College

Timothy Calvert

Electrical and Computer Engineering at California

Polytechnic State University, Pomona

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat, and
Mr. Noel Teku (Electrical and Computer Engineering)

Partners: Cameron Flores, Emily Huynh and Celyn Jacobs

Automatic Modulation Classification Using Reinforcement Learning

ABSTRACT: Automatic modulation classification (AMC) is the method of determining the modulation of a signal by trying to learn different features/properties of the received signal. AMC is useful in various civilian and military applications, such as recognizing allies and reducing overhead requirements. Many recent works have shown that different neural network architectures can be an effective tool for performing AMC. There have also been works exploring the use of AMC with equalization (i.e., filtering) to remove distortion caused by the channel. However, depending on the channel conditions, one combination of a neural network and equalizer could perform better than another. In this paper, we investigate applying reinforcement learning (RL) to a system using a blind equalizer followed by a bank of neural networks for the purpose of modulation classification. We use RL to learn/select the optimal equalizer structure and neural network for AMC.

Connor Dickey

Electrical Engineering/CyberSecurity at Bradley University

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat,
Mr. Jingcheng Li and Ms. Ziqi Xu (Electrical and Computer Engineering

Partners: Quentin Johnson and Christopher Smith

Proof-of-Following for Vehicle Platoons using a Physical Challenge-Response Protocol

ABSTRACT: Autonomous vehicle platooning promises many benefits such as fuel efficiency, road safety, reduced traffic congestion, and passenger comfort. In a typical platooning setting, vehicles travel in single file at the same speed and remain separated by the same distances. The platoon formation is autonomously maintained by a Cooperative Adaptive Cruise Control (CACC) system which fuses messages from V2X communications and sensory data (cameras, LIDAR, and radar) to navigate and maintain velocity and distance. Since messages exchanged between vehicles contain information critical to the performance and safety of the platoon, message integrity and trust between platoon members are of utmost importance. Whereas message integrity and source authentication can be verified via the PKI supported by the V2X standards, establishing the truthfulness of the information is a much harder task. In this work, we focus on the problem of proving that V2V communications for the purpose of platooning occurs only between platoon members. Specifically, we aim at tying the digital identity of a candidate vehicle requesting to join a platoon to its physical trajectory and ensure that the candidate is indeed following the platoon. Existing approaches to the following problem are susceptible to pre-recording and other attacks or are only able to bound the candidate's distance to the verifier without relative positioning and lane verification. We devise a Proof-of-Following protocol based on a physical challenge-response method whereby an existing platoon member, called the verifier challenges a platoon candidate to perturb his distance to the verifier via a random sequence of longitudinal movements. The verifier then measures such distance perturbations using its radar modality. We show that the verifier can attest that the candidate follows behind (relative positioning) at the designated platooning distance, and in the same lane.

Cameron Flores

Computer Science and Mathematics at Vassar College

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat and Mr. Noel Teku (Electrical and Computer Engineering)

Partners: Timothy Calvert, Emily Huynh and Celyn Jacobs

Automatic Modulation Classification Using Reinforcement Learning

ABSTRACT: Automatic modulation classification (AMC) is the method of determining the modulation of a signal by trying to learn different features/properties of the received signal. AMC is useful in various civilian and military applications, such as recognizing allies and reducing overhead requirements. Many recent works have shown that different neural network architectures can be an effective tool for performing AMC. There have also been works exploring the use of AMC with equalization (i.e., filtering) to remove distortion caused by the channel. However, depending on the channel conditions, one combination of a neural network and equalizer could perform better than another. In this paper, we investigate applying reinforcement learning (RL) to a system using a blind equalizer followed by a bank of neural networks for the purpose of modulation classification. We use RL to learn/select the optimal equalizer structure and neural network for AMC.

Emily Huynh

Computer Engineering at University of Nevada, Las Vegas

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat and
Mr. Noel Teku (Electrical and Computer Engineering)

Partners: Timothy Calvert, Cameron Flores, and

Celyn Jacobs

Automatic Modulation Classification Using Reinforcement Learning

ABSTRACT: Automatic modulation classification (AMC) is the method of determining the modulation of a signal by trying to learn different features/properties of the received signal. AMC is useful in various civilian and military applications, such as recognizing allies and reducing overhead requirements. Many recent works have shown that different neural network architectures can be an effective tool for performing AMC. There have also been works exploring the use of AMC with equalization (i.e., filtering) to remove distortion caused by the channel. However, depending on the channel conditions, one combination of a neural network and equalizer could perform better than another. In this paper, we investigate applying reinforcement learning (RL) to a system using a blind equalizer followed by a bank of neural networks for the purpose of modulation classification. We use RL to learn/select the optimal equalizer structure and neural network for AMC.

Celyn Jacobs

Electrical & Computer Engineering, Computer Science at University of Arizona

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat, and Mr. Noel Teku - Electrical and Computer Engineering

Partners: Timothy Calvert, Cameron Flores, and

Emily Huynh

Automatic Modulation Classification Using Reinforcement Learning

ABSTRACT: Automatic modulation classification (AMC) is the method of determining the modulation of a signal by trying to learn different features/properties of the received signal. AMC is useful in various civilian and military applications, such as recognizing allies and reducing overhead requirements. Many recent works have shown that different neural network architectures can be an effective tool for performing AMC. There have also been works exploring the use of AMC with equalization (i.e., filtering) to remove distortion caused by the channel. However, depending on the channel conditions, one combination of a neural network and equalizer could perform better than another. In this paper, we investigate applying reinforcement learning (RL) to a system using a blind equalizer followed by a bank of neural networks for the purpose of modulation classification. We use RL to learn/select the optimal equalizer structure and neural network for AMC.

Quentin Johnson

Electrical and Computer Engineering at University of Arizona

Mentors: Dr. Loukas Lazos, Dr. Michael Marefat,
Mr. Jingcheng Li and Ms. Ziqi Xu (Electrical and Computer Engineering)

Partners: Connor Dickey and Christopher Smith

Proof-of-Following for Vehicle Platoons using a Physical Challenge-Response Protocol

ABSTRACT: Autonomous vehicle platooning promises many benefits such as fuel efficiency, road safety, reduced traffic congestion, and passenger comfort. In a typical platooning setting, vehicles travel in single file at the same speed and remain separated by the same distances. The platoon formation is autonomously maintained by a Cooperative Adaptive Cruise Control (CACC) system which fuses messages from V2X communications and sensory data (cameras, LIDAR, and radar) to navigate and maintain velocity and distance. Since messages exchanged between vehicles contain information critical to the performance and safety of the platoon, message integrity and trust between platoon members are of utmost importance. Whereas message integrity and source authentication can be verified via the PKI supported by the V2X standards, establishing the truthfulness of the information is a much harder task. In this work, we focus on the problem of proving that V2V communications for the purpose of platooning occurs only between platoon members. Specifically, we aim at tying the digital identity of a candidate vehicle requesting to join a platoon to its physical trajectory and ensure that the candidate is indeed following the platoon. Existing approaches to the following problem are susceptible to pre-recording and other attacks or are only able to bound the candidate's distance to the verifier without relative positioning and lane verification. We devise a Proof-of-Following protocol based on a physical challenge-response method whereby an existing platoon member, called the verifier challenges a platoon candidate to perturb his distance to the verifier via a random sequence of longitudinal movements. The verifier then measures such distance perturbations using its radar modality. We show that the verifier can attest that the candidate follows behind (relative positioning) at the designated platooning distance, and in the same lane.

Christopher Smith

Computer Science, Mathematics at Stony Brook University

Mentored by Dr. Loukas Lazos, Dr. Michael Marefat,
Mr. Jingcheng Li and Ms. Ziqi Xu (Electrical and Computer Engineering)

Partners: Connor Dickey and Quentin Johnson

Proof-of-Following for Vehicle Platoons using a Physical Challenge-Response Protocol

ABSTRACT: Autonomous vehicle platooning promises many benefits such as fuel efficiency, road safety, reduced traffic congestion, and passenger comfort. In a typical platooning setting, vehicles travel in single file at the same speed and remain separated by the same distances. The platoon formation is autonomously maintained by a Cooperative Adaptive Cruise Control (CACC) system which fuses messages from V2X communications and sensory data (cameras, LIDAR, and radar) to navigate and maintain velocity and distance. Since messages exchanged between vehicles contain information critical to the performance and safety of the platoon, message integrity and trust between platoon members are of utmost importance. Whereas message integrity and source authentication can be verified via the PKI supported by the V2X standards, establishing the truthfulness of the information is a much harder task. In this work, we focus on the problem of proving that V2V communications for the purpose of platooning occurs only between platoon members. Specifically, we aim at tying the digital identity of a candidate vehicle requesting to join a platoon to its physical trajectory and ensure that the candidate is indeed following the platoon. Existing approaches to the following problem are susceptible to pre-recording and other attacks or are only able to bound the candidate's distance to the verifier without relative positioning and lane verification. We devise a Proof-of-Following protocol based on a physical challenge-response method whereby an existing platoon member, called the verifier challenges a platoon candidate to perturb his distance to the verifier via a random sequence of longitudinal movements. The verifier then measures such distance perturbations using its radar modality. We show that the verifier can attest that the candidate follows behind (relative positioning) at the designated platooning distance, and in the same lane.