Security for Autonomous Cyber-Physical Systems

Collin Thornton - He Bai
Oklahoma State University, Stillwater, Oklahoma, USA
Department of Mechanical and Aerospace Engineering

Introduction

Motivation:

- Remote disablement and control of Cyber-Physical Systems (CPS) is possible through external manipulation of sensory subsystems [2,3,4].
- Neural Networks (NN) are commonly used to processor sensor input on CPS.
- Traditional NN output a single-point prediction which may be untrustworthy if the input is unlike the training dataset
- Probabilistic neural networks output a variance associated with the predictive mean, alerting CPS to abnormal input.

Hypothesis:

- Probabilistic Backpropagation (PBP) [1] in NN may be used to increase the robustness of CPS against corrupted sensor input streams.

Objective:

- Explore applications of PBP NN to sensory layer of CPS
- Utilize predictive variance to gauge reliability of state estimate

Methodology

Simulation Datasets:

- Generated pure test data from Dryden Wind Model and sinusoidal wave.
- Injected datasets with normally distributed noise. Mean of 0, variable standard deviation.
- Train PBP NN and non-probabilistic NN on corrupted dataset
- Calculate RMSE based on deviation from pure dataset

Experimental Datasets:

- Measurements taken from quadrotor Unmanned Aerial System (UAS)
- UAS mounted on test stand limiting motion to rotation on one axis
- MPU6050 IMU measured inertial data on UAS
- 10k potentiometer measured ground truth rotation on test stand
- 5 samples with motors off, 3 with motors on
  - 1 sample ~1200 points over ~60 seconds
- Train PBP NN and MATLAB NN on datasets with motors on
- Calculate RMSE based on deviation from ground truth data.

Results

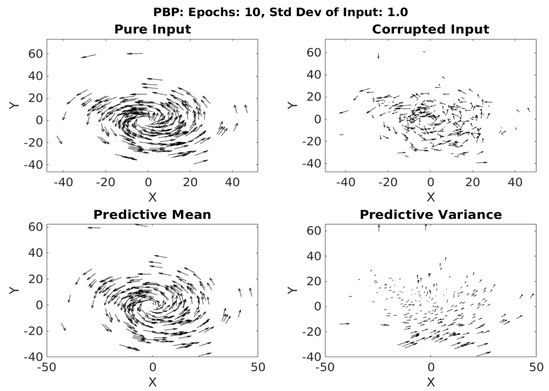

Figure 1: PBP NN on Dryden Wind Model $+\lambda,\ \lambda \sim \mathcal{N}(0,1)$
RMSE: 0.1602

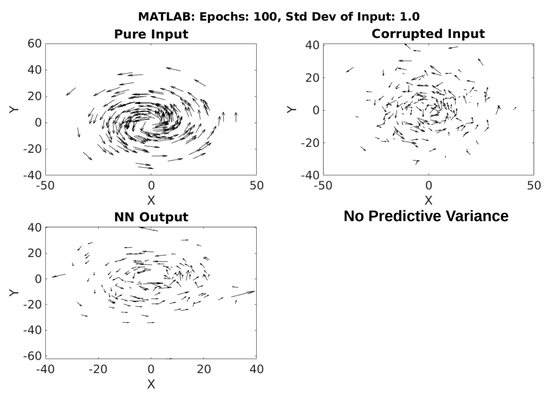

Figure 2: MATLAB NN on Dryden Wind Model $+\lambda, \lambda \sim \mathcal{N}(0,1)$
RMSE: 0.9451

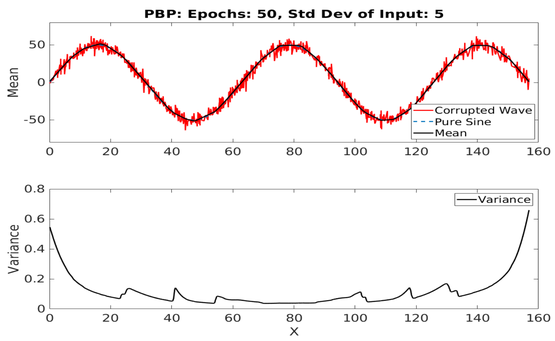

Figure 3: PBP NN on $y = 50sin(x) + \lambda,\ \lambda \sim \mathcal{N}(0, 5^2)$
RMSE: 0.6044

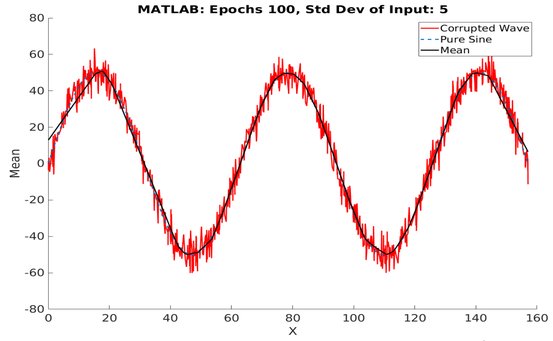

Figure 4: MATLAB NN on $y = 50sin(x) + \lambda,\ \lambda \sim \mathcal{N}(0, 5^2)$
RMSE: 2.1195

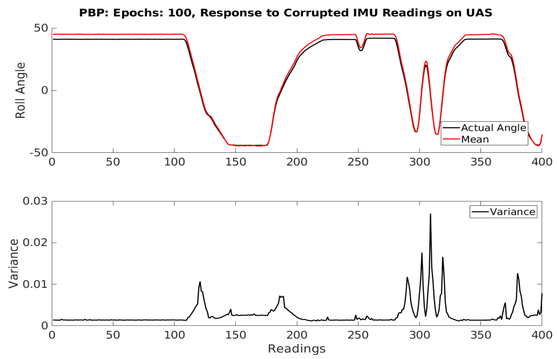

Figure 5: PBP NN on Poorly Calibrated MPU6050 IMU
RMSE: 3.0661

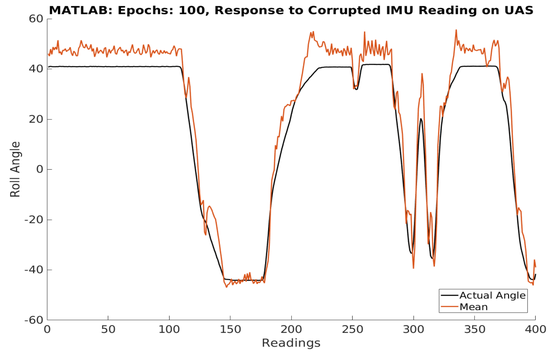

Figure 6: PBP NN on Poorly Calibrated MPU6050 IMU
RMSE: 7.8345

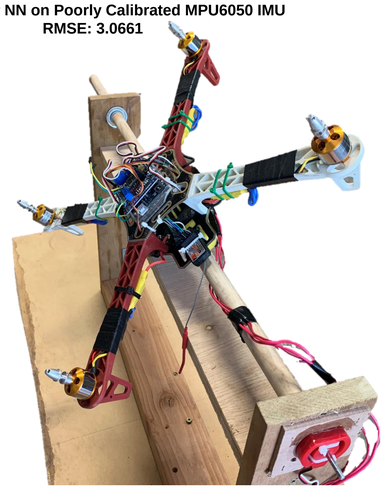

Figure 7: UAS Test Stand

Discussion

Neural Networks:

- Used to approximate arbitrary functions
- Commonly implemented when an explicit function is difficult to define
- Loosely modeled after the human brain, utilizing perceptrons to make unit decisions

PBP NN:

- Algorithm developed by [1]
- Utilizes a Bayesian NN
- Generates point mean and estimate of model reliability in the posterior uncertainty of weights

Figures 1,2:

- Trained on 10,000 datapoints.
- PBP performed with smaller RMSE after 1/10 training epochs

Figures 3,4:

- Trained on 10,000 datapoints
- PBP performed with 1/3 the RMSE of MATLAB NN after ½ training epochs

Figures 5,6:

- Trained on ~3200 datapoints with motors at 100%
- PBP much better at filtering acoustic vibrations
- Predicted variance was ~2x that of properly calibrated samples

Figure 7:

- UAS test stand built to limit rotation to roll axis

Conclusions

Conclusions:

- PBP NN are much better at handling normal distributions than similar non-probabilistic NN.
- This is beneficial in processing sensor input
- Estimates of the posterior uncertainty of weights provided by PBP useful as gauge of network confidence

Future Work:

- Increase sample size of dataset
- Include multiple sensor streams
- Test PBP on multiple probability distributions

[1] J. Hernández-Lobato, and R. Adams. “Probabilistic Backpropagation for Scalable Learning of Bayesian Neural Networks”. *arXiv*:1502:05336v2 [stat.ML]. 2015
[2] W. Chen, Y. Dong, and Z. Duan. Manipulating drone dynamic state estimation to compromise navigation. In *2018 IEEE Conference on Communications and Network Security (CNS)*, page 1-9. May 2018.
[3] Y. Son, H. Shin, et al. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 881-896, Washington, D.C., 2015. USENIX Association
[4] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu. Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *2017 IEEE European Symposium on Security and Privacy (EuroS P),* pages 3-18, April 2017.