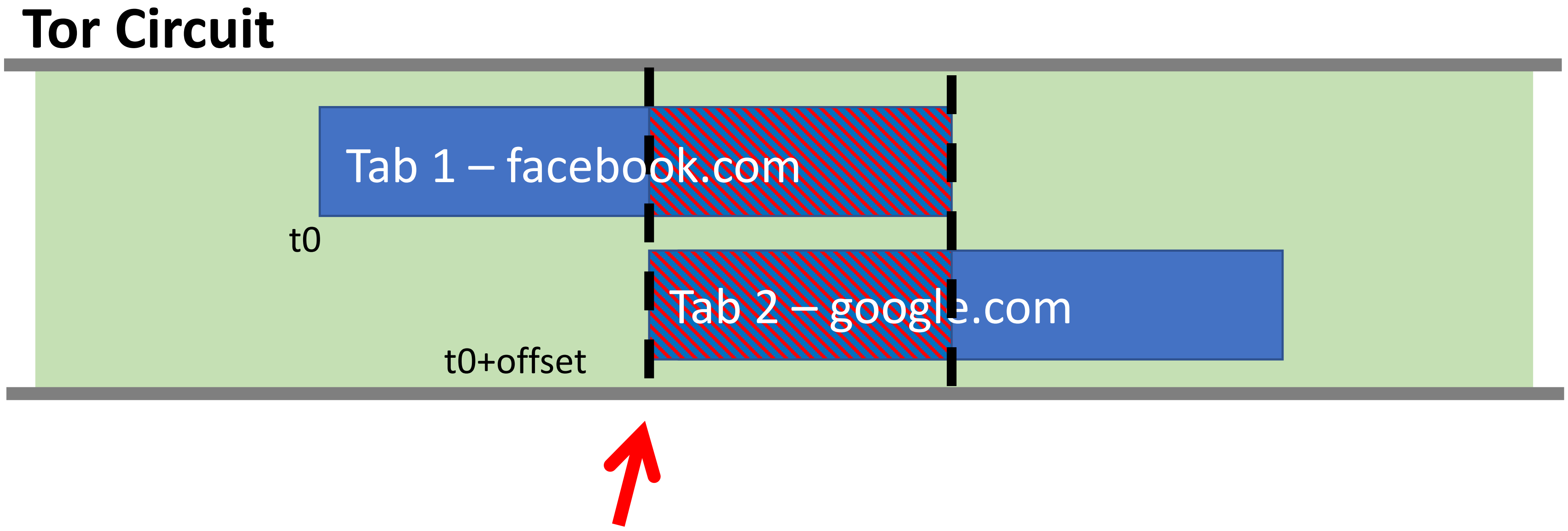
Multi-tab (review)



Predict this point

Hypothesis

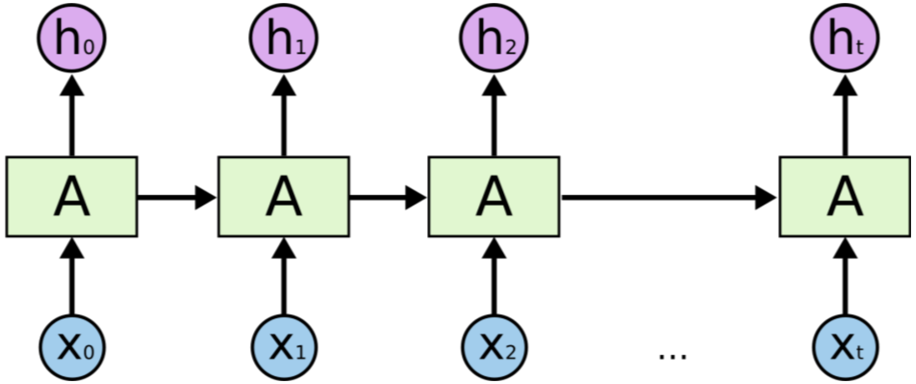
H1: Deep learning techniques improve the performance of multi-tab sample splitting when compared to the hand-crafted feature-based techniques from prior works.

H2: Multi-tab Website Fingerprinting attack performance can be shown to be comparable to attack performance in the Single-Tab.

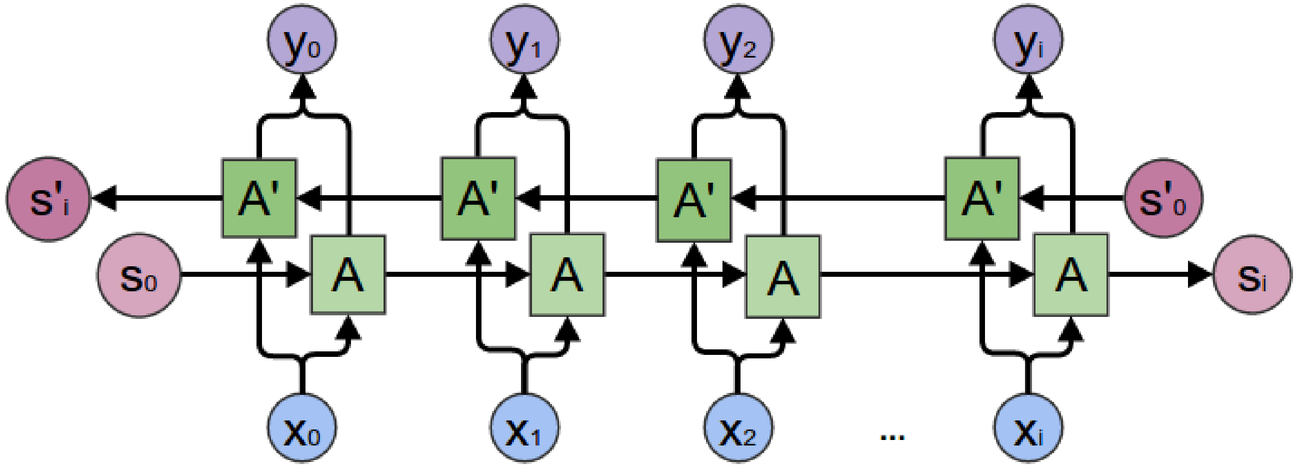
Nate Mathews, nate.mathews@mail.rit.edu

LSTMs Quick Review

Basic LSTM

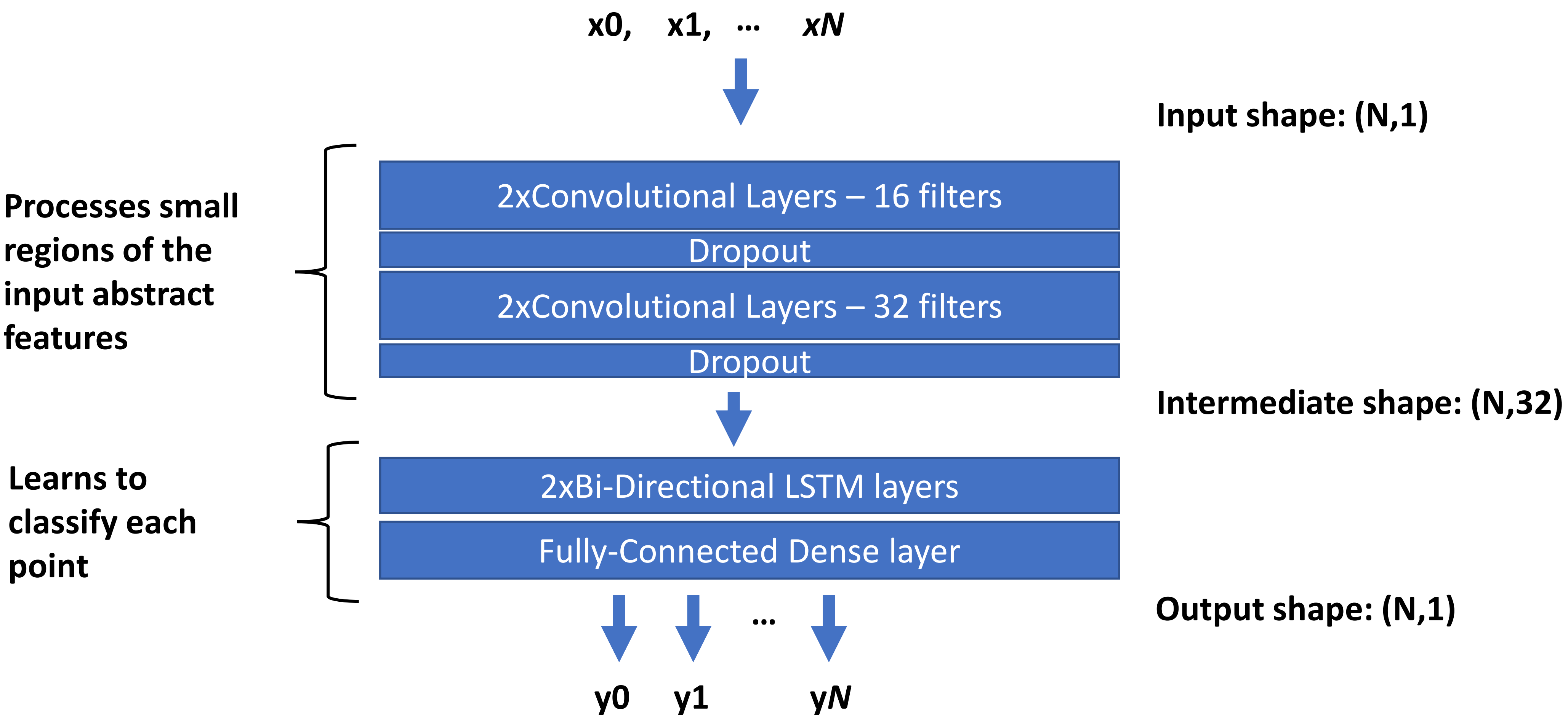


Bi-Directional LSTM



CNN-BiLSTM

x -> *packet_time * packet_direction*



x0, x1, … *xN*

Input shape: (N,1)

Processes small regions of the input abstract features

2xConvolutional Layers – 16 filters

Dropout

2xConvolutional Layers – 32 filters

Dropout

Intermediate shape: (N,32)

Learns to classify each point

2xBi-Directional LSTM layers

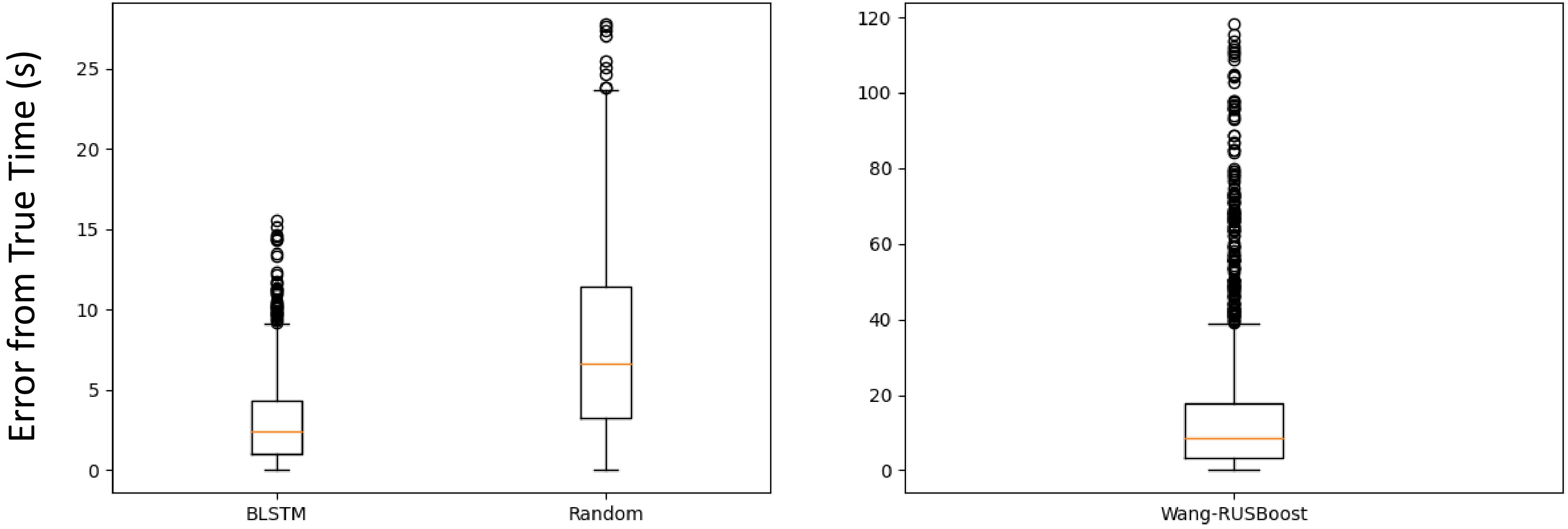
Fully-Connected Dense layer

Output shape: (N,1)

y0 y1 … y*N*

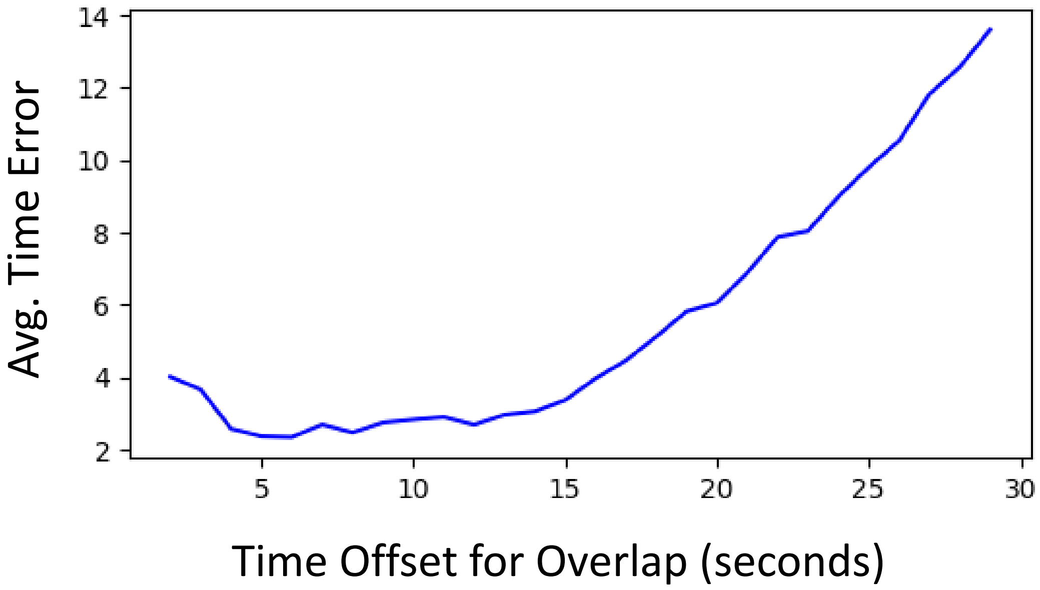
Sample Splitting Evaluations

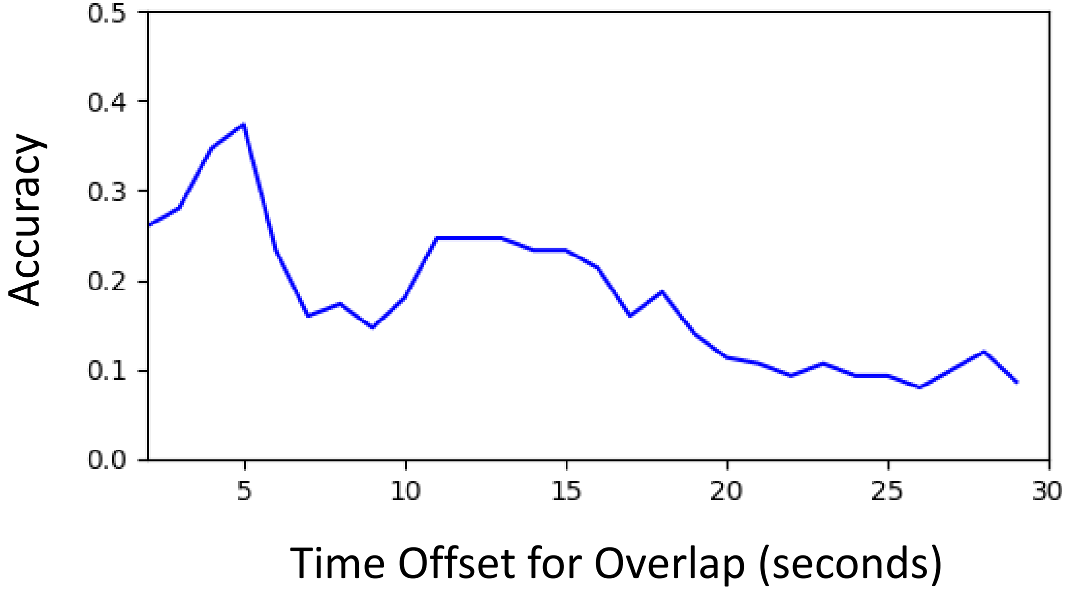
	CNN-BiLSTM	[1] Features	Random
Accuracy (Counted correct if within 25 packets)	25.2%	14.9%	2.7%



Sample Splitting Evaluations

- Performance at different overlap offsets

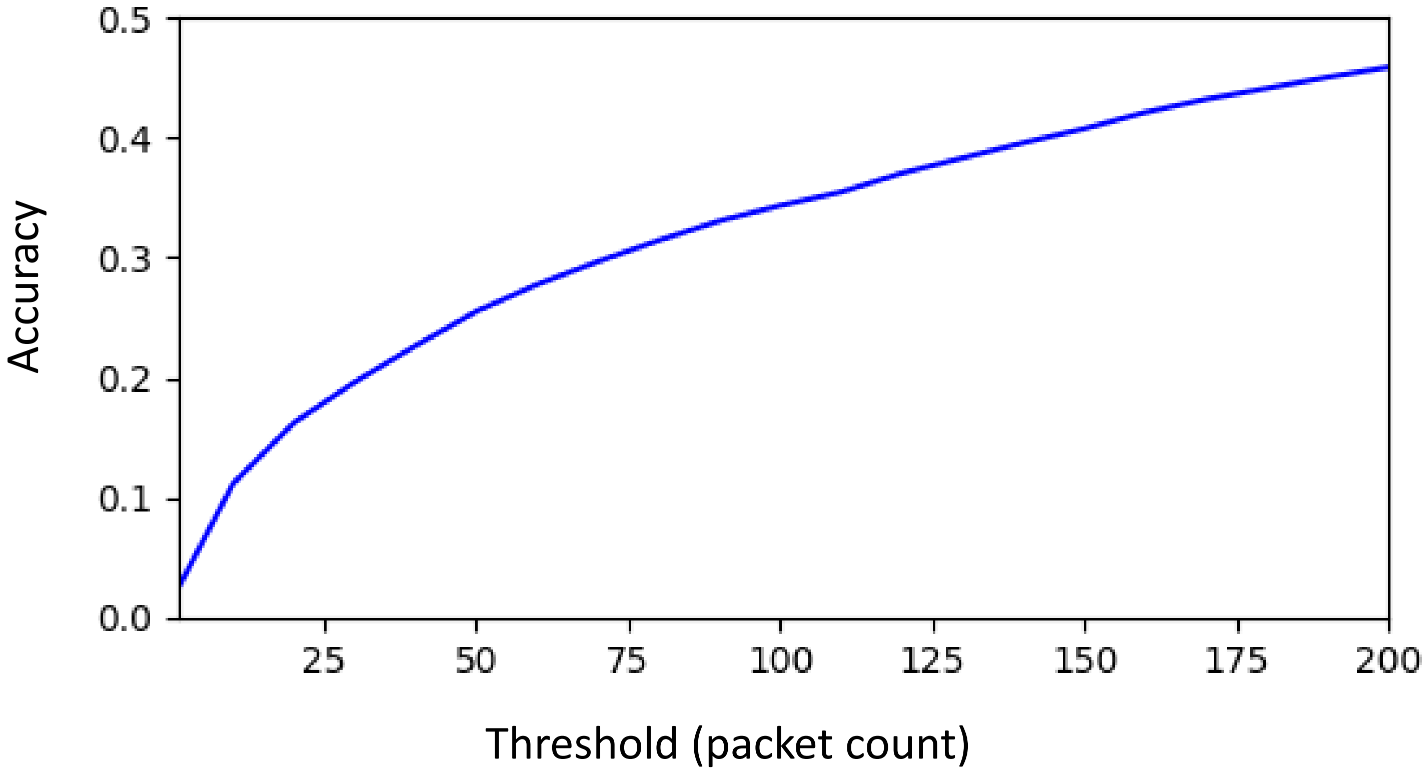




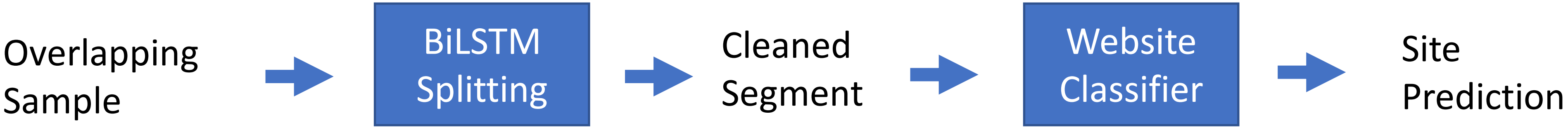
Nate Mathews, nate.mathews@mail.rit.edu

Sample Splitting Evaluations

- Performance at different packet threshold values
  (prediction counted as correct if within *threshold* packets)



Is this useful? Classifying Split Samples



Using CNN Website Classifier from … [CCS'18] Sirinam et al. "*Deep Fingerprinting: Undermining Website Fingerprinting Defenses with Deep Learning*"

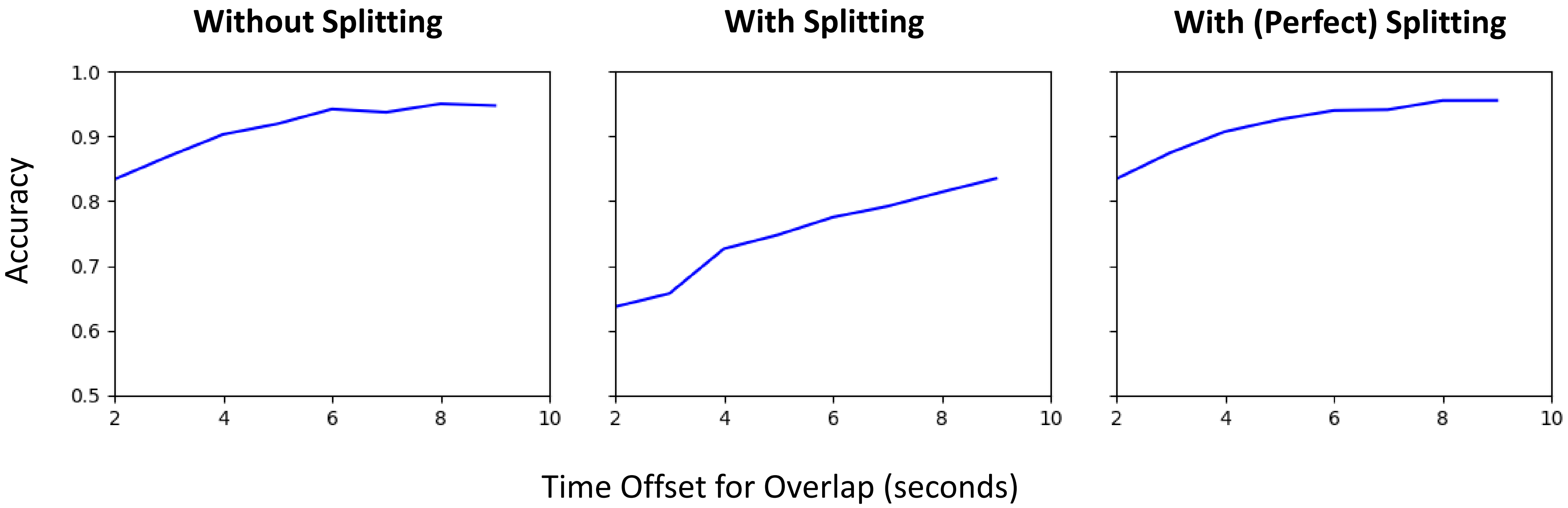
Data representation is ***x*** = *time_stamp * direction*

Without Splitting	With Splitting	With (simulated) Perfect Splitting
91.2%	74.8%	91.6%

+ Single-Tab ~96% accuracy

Classifying Split Samples

- Performance at different overlap offsets



Without Splitting

With Splitting

With (Perfect) Splitting

Conclusions so far…

H1: Deep learning techniques improve the performance of multi-tab sample splitting when compared to the hand-crafted feature-based techniques from prior works.

Yes!

H2: Multi-tab Website Fingerprinting attack performance can be shown to be comparable to attack performance in the Single-Tab.

Yes, but actually no

To Do:

- Simulate 3+ tabs to make it more difficult for the CNN
- Transfer learning to improve splitting model