CAMLIS 2022: Temporal Attack Detection in Multimodal Cyber-Physical Systems with Sticky HDP-HMM

Dr. Andrew E. Hong, Peter M. Malinovsky, and Dr. Suresh Damodaran

Approved for Public Release; Distribution Unlimited.
Public Release Case Number 22-2488.

October 21, 2022

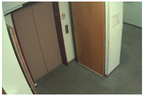
MITRE

Cyber-physical Systems



Platform Control & Autonomy

SCADA



Sensors

IoT




[1] Image sources:
https://www.navy.mil/strategic/Naval_Aviation_Vision.pdf
https://www.imef.marines.mil/Photos/igphoto/151202/

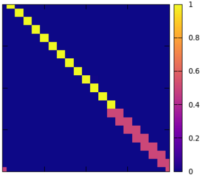
Background & Motivation

- Problem: automatically identify attack events in time series
- Definite & total knowledge of ‘normal behavior’ absent
- Many cyber-physical systems (CPS) are multi-modal: what’s “normal in one mode is ‘abnormal’ in another”
- Learning problem to infer the natural number of modes

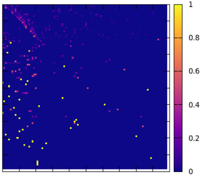
Background & Motivation (cont.)

- CPS produce a wealth of heterogeneous data: continuous (e.g. altitude, pressure), ordinal (e.g. floor number), nominal (e.g. commands, messages)
- Manual feature extraction remains the standard practice, but is costly & time-consuming
- Bayesian model-based approach able to extract these events from many forms of signals

States & Transitions



(a) Regular Transitions



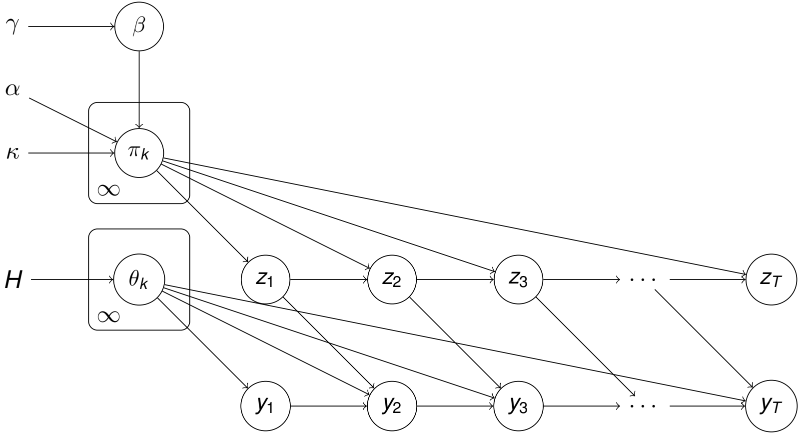
(b) Anomalous Transitions

Modified Sticky Hierarchical Dirichlet Process Hidden Markov Model

- Inference on the latent state labeling z_t is how event transitions are determined
- Each latent state i has an associated collection of sufficient statistics or parameters θ_i

Global Dirichlet	$\beta \mid \gamma$	$\sim \text{GEM}(\gamma)$	$i = 1, \ldots$
Process Prior:	θ_i	$\sim H$	
Transition Matrix Prior:	$\pi_{i,\cdot}$	$\sim DP(\alpha \cdot \beta + \kappa \cdot \delta_i)$	$i = 1, \ldots$
Latent State Transition:	$z_t \mid z_{t-1}$	$\sim \pi_{z_{t-1},\cdot}$	$t = 1, \ldots, T$
Configuration Transition Prior:	$y_t \mid y_{t-1}, z_{t-1}, p^{z_{t-1}}$	$\sim p^{z_{t-1}}_{y_{t-1}, y_t}$	$t = 1, \ldots, T$

Modified Sticky Hierarchical Dirichlet Process Hidden Markov Model (cont.)



MITRE

Inference Algorithm

Algorithm 1: Direct Assignment Gibbs Sampler for sHDP-HMM

for $i = 1, \dots, n$ **do**

  for $t = 1, \dots, T$ **do**

    Decrement $N[z_{t-1}^{(i)}, z_t^{(i-1)}]$, $N[z_t^{(i-1)}, z_{t+1}^{(i-1)}]$

    Sample the state labeling $z_t^{(i)}$

    if $z_t^{(i)} = K^{(i)} + 1$ **then**

      Introduce state $K^{(i)} + 1$ into array $\beta^{(i)}$ and matrix N

      Increment $K^{(i)}$

    Increment $N[z_{t-1}^{(i)}, z_t^{(i)}]$, $N[z_t^{(i)}, z_{t+1}^{(i-1)}]$

  for $j = 1, \dots, K^{(i)}$ **do**

    if $N_{j\cdot} = 0$ *and* $N_{\cdot j} = 0$ **then**

      Delete row and column j from N

  Update the count of unique states $K^{(i)} = |j : z_t^{(i)} = j \text{ for } t = 1, \dots, T|$

  Sample the CRF auxiliary variable matrix $M^{(i)}$

  Sample the self-transition parameter(s)

  Sample the global weights $\beta^{(i)}$

  Sample the hyper-parameters

MITRE

Avionics Testbed

- MIL-STD-1553, serial bus communication protocol standard, testbed
- Remote terminal (RT) components interact with common master device - bus controller (BC) through Alta eNet interface
- For example, GPS receivers, auto-pilot controllers, or flight control components such as ailerons, elevators, and rudders
- Attacks conducted on components, analyzed messages sent/received by the bus controller

Message Type	Remote Terminal Address	Transmit/Receive	Subaddress	Mode Code

MITRE

Avionic Testbed 1553 Bus Traffic Experiments

Satellite 1553 Bus Experiments				
Attack	***Attack Occurrence***	***Detected Occurrence***	***Detection***	***Description***
Attack 0	3451 - 4248	3451 - 4248	TP	Denial of Service 1
Attack 1	4538	4538	TP	Noise Attack 1
Attack 2	4568	4568	TP	Noise Attack 2
Attack 3	4714	4714	TP	Noise Attack 3
Attack 4	4860	4860	TP	Noise Attack 4
Attack 5	5006	5006	TP	Protocol Violation 1
Attack 6	5152	5152	TP	Protocol Violation 2
Attack 7	5298	5298	TP	Protocol Violation 3
Attack 8	5444	5443 - 5445	TP	Protocol Violation 4
Attack 9	5590 - 5968	5600, 5647-5700, 5740-5745, 5773-5789, 5818-5834, 5863-5879, 5908-5911	TP	Denial of Service 2
Attack 10	6114	6114	TP	Buffer Attack 1
Attack 11	6405	6405	TP	Buffer Attack 2
Attack 12	6551	6551	TP	Anomalous Traffic 1
Attack 13	N/A	N/A	FN	Atypical Traffic
Attack 14	6726	None	FN	Anomalous Traffic 2
Attack 15	6872	6872	TP	Anomalous Traffic 3
Attack 16	7018	7018 - 7019	TP	Data Payload Attack

MITRE

iRobot Create® 2

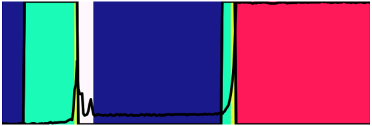
- iRobot consumer product
- Consider two kinds of attacks:
  1. Blocking wall sensors
  2. Obstructing tires

[1] Image source: https://edu.irobot.com/what-we-offer/create-robot

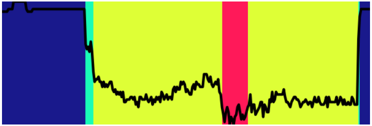
iRobot Create® 2 Experiments (cont.)

(a) Wall sensors and states under normal operation.

(b) Current readings and states under normal operation.



(c) Wall sensors and states under sensor attack.



(d) Current readings and states under actuator attack.

MITRE

iRobot Create® 2 Experiments

Roomba Experiments			
Experiment	***Attack Vector***	***Data***	***Attack Occurrence***
1	wall sensors	light bumpers, velocity	(58, 59) - (74, 75)
2	actuators	current, voltage	(171, 172) - (212, 217)
Experiment	***Detected Occurrence***	***Start Attack***	***End Attack***
1	62 - 73	TP	TP
2	172 - 192	TP	FN

MITRE

MITRE is a not-for-profit organization whose sole focus is to operate federally funded research and development centers, or FFRDCs. Independent and objective, we take on some of our nation's—and the world's—most critical challenges and provide innovative, practical solutions. Learn and share more about MITRE, FFRDCs, and our unique value at

https:\www.mitre.org