Time Intervals as a Behavioral Biometric

John (Vinnie) Monaco

Seidenberg School of CSIS, Pace University

November 11, 2015

http://vmonaco.com/dissertation

Outline

"You are ~~what~~ *when* you eat"

Newell's time scale.

Newell's time scale of human action

Scale (sec)	Time Units	System	World (theory)
10^{7}	Months		**SOCIAL BAND**
10^{6}	Weeks		
10^{5}	Days		
10^{4}	Hours	Task	**RATIONAL BAND**
10^{3}	10 min	Task	
10^{2}	Minutes	Task	
10^{1}	10 sec	Unit task	**COGNITIVE BAND**
10^{0}	1 sec	Operations	
10^{-1}	100 ms	Deliberate act	
10^{-2}	10 ms	Neural circuit	**BIOLOGICAL BAND**
10^{-3}	1 ms	Neuron	
10^{-4}	100 µs	Organelle	

Behavioral biometrics.

The measure of human behavior for the purpose of identification or verification.

Timestamped events and time intervals.

- Timestamped events: keystrokes, touchscreen gestures, financial transactions, source code contributions...
- Given a series of events that occur at times $t_0, t_1, \ldots, t_N$

Time interval between events

$$\tau_n = t_n - t_{n-1}$$

Outline

1. Introduction
   - Motivation
   - Background
2. Data
   - Description
   - Empirical patterns
3. Modeling
   - Model specification
   - Experimental results
4. Conclusions

Why focus on timestamps?

- Timestamps are truly ubiquitous
- Timestamps are persistent
- Timestamps are resilient to encryption and masking
- Timestamps can generally be collected without cooperation
- Timestamps can be incorporated into domain-specific models

Problems.

Identification Given a sequence of events, decide who they belong to (1 out of N)

Verification Given a sequence of events with claimed responsibility, decide whether the claim is legitimate (binary classification)

Prediction Given a sequence of events, predict the time of a future event

Outline

1. Introduction
   - Motivation
   - Background
2. Data
   - Description
   - Empirical patterns
3. Modeling
   - Model specification
   - Experimental results
4. Conclusions

Bursts of activity in human behavior.

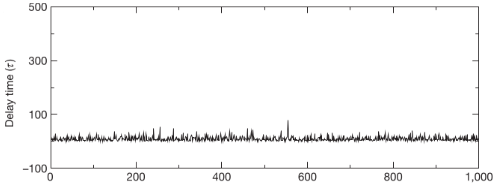
Random process (Poisson process, exponential inter-event times)

Bursty process (power-law inter-event times)

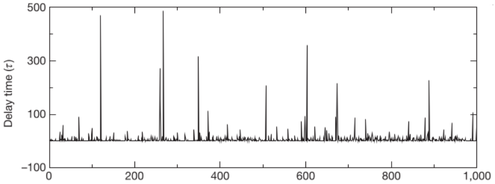
Barabasi, 2005

Time intervals of a random vs. bursty process.

Random process



Bursty process

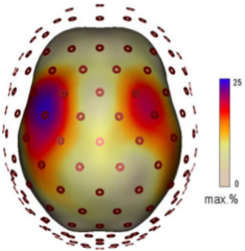


Barabasi, 2005

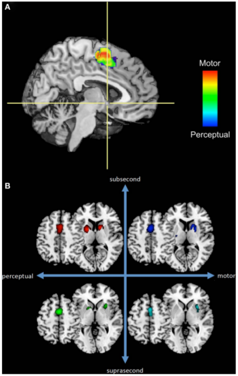
Psychology of human timing.

Implicit and explicit timing

Neurophysiology of human timing.



Praamstra, 2006



Wiener, 2011

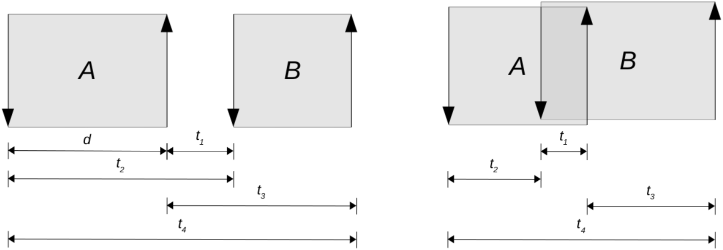
Outline

1. Introduction
   - Motivation
   - Background
2. Data
   - Description
   - Empirical patterns
3. Modeling
   - Model specification
   - Experimental results
4. Conclusions

Datasets.

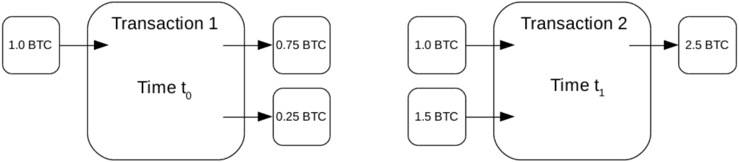
Dataset	Source	Size	Freq.(Hz)
Keystroke fixed-text	Monaco et al. (2013)	24k keystrokes, 60 users	4.4
Keystroke free-text	Villani et al. (2006)	251k keystrokes, 56 users	3.8
Mobile	Jain et al. (2014)	11k gestures, 52 users	3.1
Keypad	Bakelman et al. (2013)	6.6k keystrokes, 30 users	2.9
Bitcoin transactions	Reid et al. (2013)	239k transactions, 61 users	2.8×10^{-4}
Linux kernel commits	Passos et al. (2014)	16k commits, 52 authors	2.6×10^{-6}
White House visits	Hudson (2015)	2.7k visits, 18 people	1.4×10^{-6}
Terrorist events	LaFree et al. (2007)	1.8k events, 10 groups	2.8×10^{-7}

Keystroke.



Non-overlapping and overlapping keystrokes

Bitcoin transaction.



Terrorist activity.

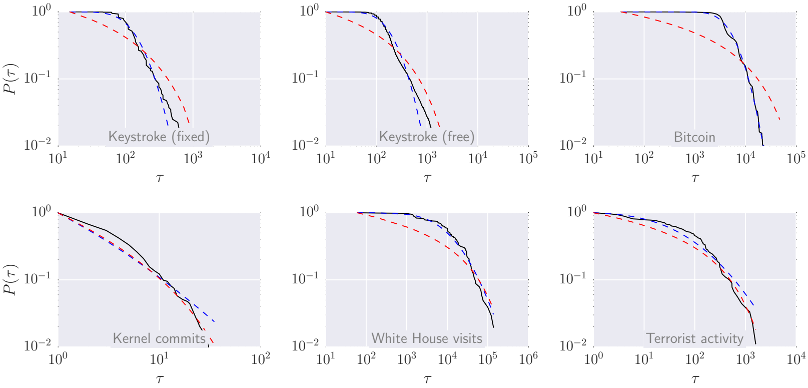
GTD GLOBAL TERRORISM DATABASE

START

NATIONAL CONSORTIUM FOR THE
STUDY OF TERRORISM AND RESPONSES TO TERRORISM

Outline

Heavy tails.

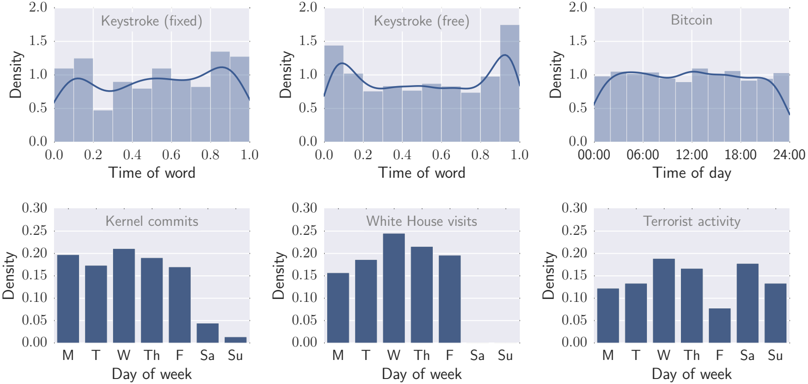

Keystroke (fixed)
Keystroke (free)
Bitcoin
Kernel commits
White House visits
Terrorist activity
$P(\tau)$
τ

Preference for a log-normal.

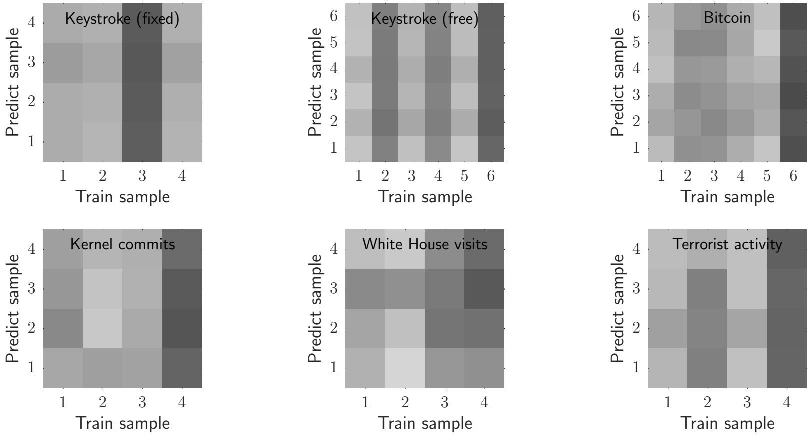
Power law vs log-normal loglikelihood ratio tests

Dataset	Power law	Log-normal
Keystroke (free)	0.00 (0.00)	1.00 (1.00)
Keystroke (fixed)	0.00 (0.00)	1.00 (1.00)
Bitcoin	0.00 (0.00)	1.00 (1.00)
Kernel commits	0.75 (0.56)	0.25 (0.08)
White House visits	0.00 (0.00)	1.00 (1.00)
Terrorist activity	0.70 (0.20)	0.30 (0.00)

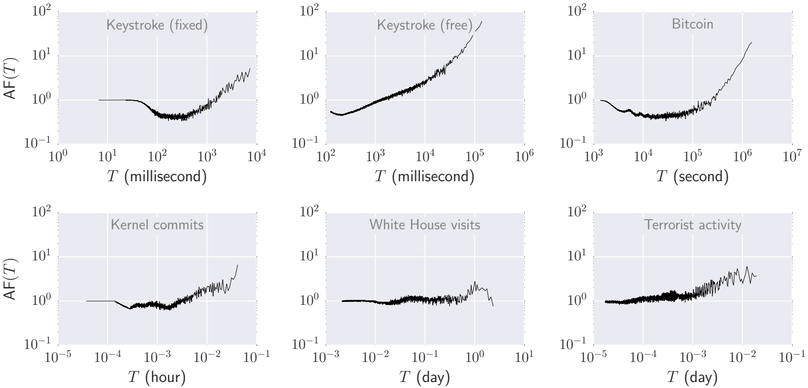
Time dependence.



Non-stationarity.



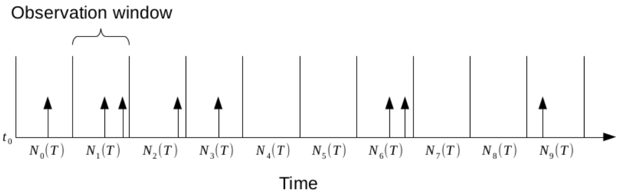
Temporal clustering.



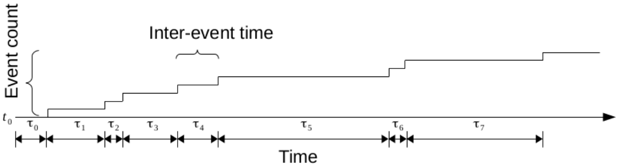
Outline

1. Introduction
   - Motivation
   - Background
2. Data
   - Description
   - Empirical patterns
3. Modeling
   - Model specification
   - Experimental results
4. Conclusions

Modeling approaches.



Windowed observations and event intensity



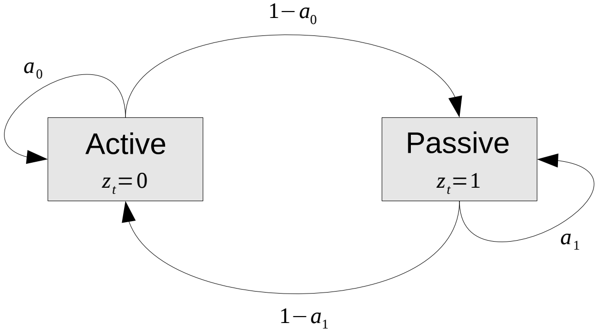
Time interval observations and event count

Time interval distribution.

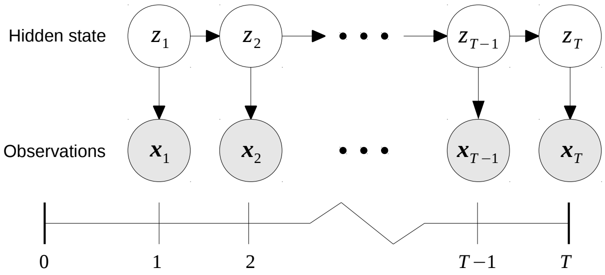
Log-normal

$$f(\tau;\mu,\sigma) = \frac{1}{\tau\sigma\sqrt{2\pi}} \exp\left(\frac{-(\ln\tau-\mu)^2}{2\sigma^2}\right) \quad \tau > 0$$

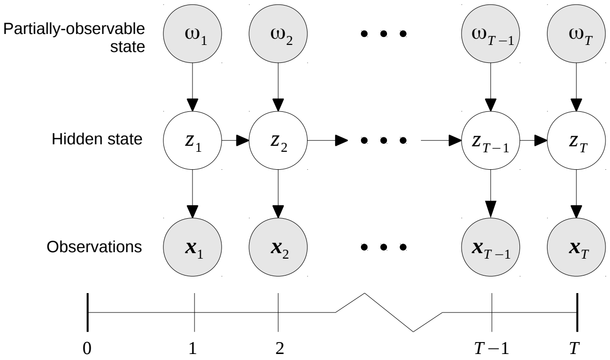
Transitioning between hidden states.



Hidden Markov model.



Partially-Observable Hidden Markov Model.



POHMM as an extension to the HMM.

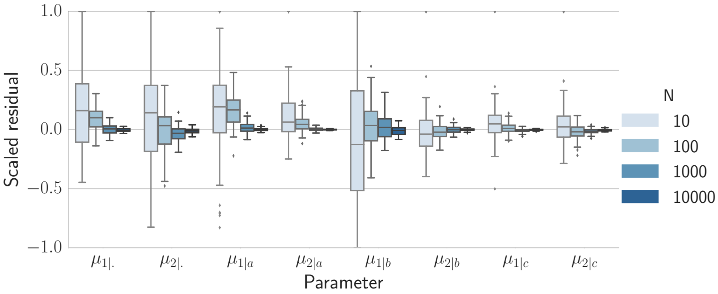
- Introduces a dependency into the HMM to account for event *types* (e.g., key names).
- Can handle missing or incomplete observations by using the marginal distributions.
- Avoids overfitting through parameter mixing (or smoothing).

Consistency.

To be consistent the model must be:

- Convergent
  - Will our estimator always converge to a value?
- Asymptotically unbiased
  - Given a sample generated from a model with known parameters, can we recover the model parameters as the size of the sample increases?

Residuals.

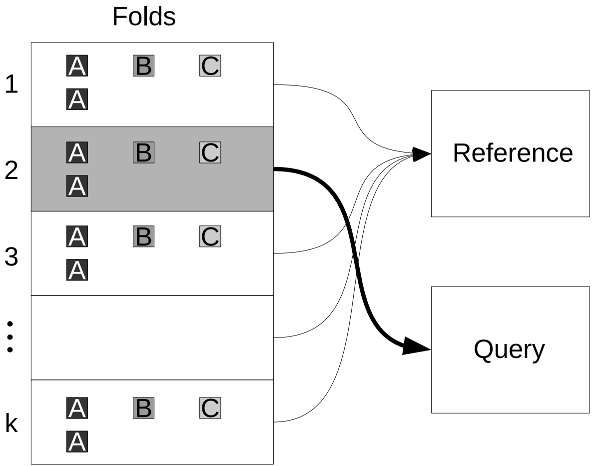

1.0
0.5
0.0
−0.5
−1.0
Scaled residual
$\mu_{1|.}$
$\mu_{2|.}$
$\mu_{1|a}$
$\mu_{2|a}$
$\mu_{1|b}$
$\mu_{2|b}$
$\mu_{1|c}$
$\mu_{2|c}$
Parameter
N
10
100
1000
10000

Outline

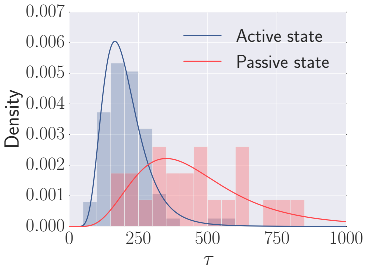
Evaluation criteria.

- Identification: rank-1 classification accuracy (ACC).
- Verification: equal error rate (EER), the point on the ROC curve where $P(\text{false accept}) = P(\text{false reject})$.
- Continuous verification: average maximum rejection time (AMRT), the average number of events before an impostor is detected without falsely rejecting the genuine user.

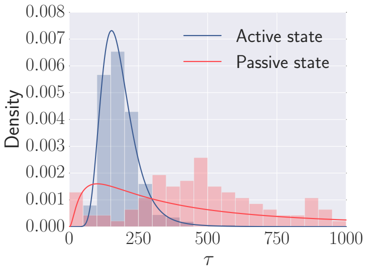
Evaluation procedure.



Fitted model example.



Fixed-text

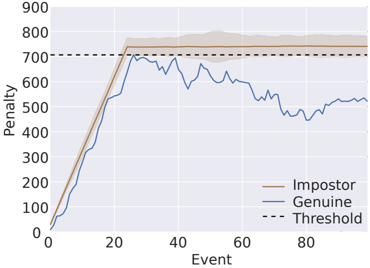


Free-text

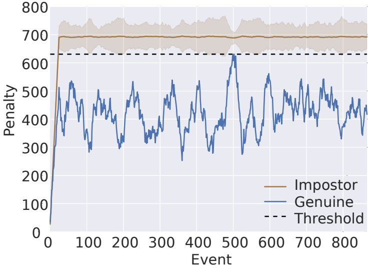
Keystroke experimental results.

	Folds	Dichotomy	POHMM	p-value
Nursery rhymes	4	0.11 (0.04)	**0.00** (0.01)	0.003
Keystroke (fixed)	4	0.13 (0.02)	**0.08** (0.04)	0.041
Keystroke (free)	6	**0.02** (0.01)	0.06 (0.01)	8.9×10^{-5}
Keypad	20	0.11 (0.03)	**0.05** (0.02)	1.3×10^{-8}
Mobile (w/o sensors)	20	0.20 (0.03)	**0.10** (0.02)	2.7×10^{-14}
Mobile (w/ sensors)	20	0.01 (0.01)	0.01 (0.01)	0.500

Continuous verification.



Fixed-text



Free-text

Bitcoin experimental results.

- Hidden states are partially observable through the transaction direction (*incoming* or *outgoing*).
- 0.42 ACC
- 0.14 EER
- 139 AMRT

Linux kernel commit experimental results.

- Hidden states are partially observable through the commit intention (*bug fix* or *feature addition*).
- 0.17 ACC
- 0.36 EER
- 41 AMRT

White House visit experimental results.

- Hidden states are partially observable through the size of the group (*small* or *large*).
- 0.31 ACC
- 0.28 EER
- 19 AMRT

Terrorist activity experimental results.

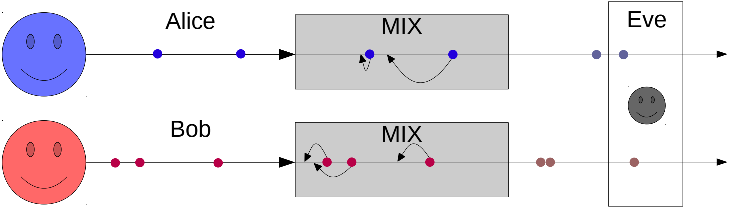
- Hidden states are partially observable through the *group intention*.
- 0.15 ACC
- 0.45 EER
- 37 AMRT

What about anonymity?

- Timestamps can reveal your identity.
- Encryption, VPN, TOR, etc., cannot prevent that.

Masking temporal behavior.

Alice and Bob want to be anonymous.

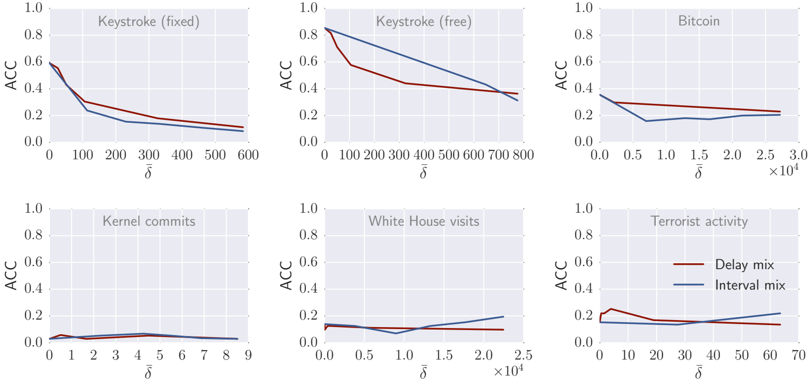


Masking strategy properties.

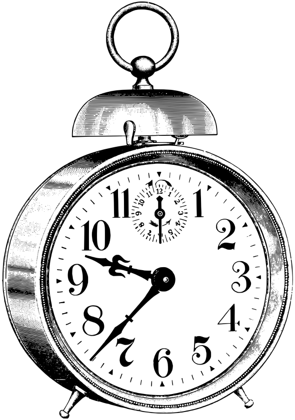
Finite	The expected delay between the user and the arrival process should not grow unbounded.
Anonymous	The mix should make it difficult to identify the user.
Unpredictable	The mix should make it difficult to predict future behavior.

Proposed mixing strategies experimental results.

Masking capability increases as the tolerable lag increases.



Conclusions.



Questions.

Thank you