A Bayesian decision support system for counteracting activities of terrorist groups

Jim Smith, Aditi Shenvi & Oliver Bunnin,

University of Warwick & Alan Turing Institute

June 2022 Montreal ISBA

Co-creating Criminal models: using Bayes as a language

- For data rich dynamic processes **subjective expert judgements** are needed both to **fill in** inevitable gaps & to bring **focus**.
- For real time Bayesian decision support the **models need to be open** to receive unanticipated expert knowledge.
- Graphs excellent tools for guiding accommodation of expert knowledge - but these **graphs and their semantics are best customised to the application in hand** Wilkerson &S (21).
- When knowledge is embedded through latent, not directly observed, states we **need no data - nor even knowledge of the precise nature of measurement variables** - to transfer model to a sensitive inhouse domain.

Using Shenvi et al,22: illustrate process of building a Bayesian model with customised graph - here to support pursuit of gangs plotting violent attacks against general public.

Co-creating Bayesian models of behaviour of criminals

- **Bespoke graphical models** guide structure domain judgements - communicated in natural language $\longrightarrow$ a probability model $\longrightarrow$ integrating data with domain knowledge.
- For POI's "expert judgements" about **individuals** concern:
  1. Genesis of **criminal life paths** (sociologists, criminologists, police).
  2. **Case files** of specific individuals (various).
  3. **Real time activity** data about this suspected plot (surveillance).
- Expert judgements elicited about potential **formation, coordination & collaboration across gang members**.
  1. **Skills** & **scope** for the crime (sociologists, criminologists, police)
  2. Known **strength of associations** between specific individuals (police)
  3. **How** different POI's are **communicating now** (surveillance).
- Expert judgements to score **threat** posed by different gangs (police).

Individual model of POI: component 1

Elicitations $\Rightarrow$ $\boxed{\text{New class of } \textbf{RDCEG} \text{ (Shenvi \& S,19, Shenvi, 21)}}$

- RDCEG **classifies potential latent trajectories of RVEs** before arrest & conviction.
- Translates these into predictive stochastic models in **formal, explainable & auditable** way.

So put more technically:

- Depict deepest layer as family of **time inhomogeneous semi-Markov processes (RDCEGs)**.
- Builds a **3 level Bayesian hierarchical model**: a Bayesian Dynamic Linear Markov Switching Model $\longrightarrow$ select & accommodate streaming data.

A Lone Suspect Planning an Attack: Real Time Support

- Triaged ω suspected of planning & perpetrating **attack on the public**.
- To succeed ω needs to perform a set of **tasks** - possibly undertaken in variety of ways.
- Police see a high dim. (informedly censored) **observation vector time series** $\{\mathbf{Y}_t\}_{t \geq 0}$ about ω, e.g. of movements in space & time, web hits, meta data from phone messages how long & to whom,... multiple sources.

Notes

1. Single **tasks** do not usually define stages of criminal preparation. HOWEVER **in combination highly indicative**.
2. Best tasks = activities **surprising for innocent person** to engage in.

The Generic Three level hierarchy

Processes of individuals' journeys within particular plot

Bayesian Hierarchical Model	Components	Symbol
*	*	*
Data sources we have sight of	tell-tale signs	$\{\mathbf{Z}_t\}_{t\geq 0}$
$\uparrow$		
Tasks associated to phases of plot	logic/background	$\{\boldsymbol{\theta}_t\}_{t\geq 0}$
$\uparrow$		
Phases representing phases of plot	criminology	$\{\mathbf{W}_t\}_{t\geq 0}$

A Bespoke Decision Support Tool for Pursuing RVEs

Special challenges of this domain:

1. **Very dynamic** & subject to controls.
2. Essential dynamics often **hidden** - data just gives glimpses of what might be happening.
3. **Open model**: police need to **intervene & adapt** system **to sporadic external new information**.
4. Must **filter** vast streaming data about suspect so needs filtering.
5. **Data** - dynamic, patchy, informedly censored, indirectly inform latent stages.
6. Guide **development** of inhouse system **securely** for such refined models.

All possible if building a subjective Bayesian model!

A Hierarchical Dynamic Model of a Violent Suspect

Example

Bomb attack must *know how to make bomb* $\Leftarrow z$ taught/search web/. *Acquire ingredients for bomb* $\Leftarrow z$ seen buying/receiving/stealing. *Identify target* - its defenses & demographics $\Leftarrow z$ visit/electronically explore maps./contacts for planning. *Travel to target site* $\Leftarrow z$ moves monitored with CCTV, tagged, reported seen.

MORE GENERICALLY

- **Deepest level** RDCEG: unfolding intent - transitions between threat positions w_i at time t, $i = 1, 2, \ldots, n$.
- **Intermediate level** a vector of **Tasks** $\boldsymbol{\theta}_{I(w_i),t}$ ω likely to do if at position w_i.
- **Surface level** an intensity measure of activities z_{it} at time t associated with task $\theta_{i,t}$.

DBN of overarching process with an example time slice

$$
\begin{array}{lccccccc}
\text{Raw time vectors} & & & & \mathbf{Y} & & & \\
 & & & \nearrow & \uparrow & \nwarrow & & \\
\text{Intensity vector} & & Z_{t-1} & & Z_t & & Z_{t+1} & \text{tell tale signs} \\
 & & \uparrow & & \uparrow & & \uparrow & \\
\text{Task vector} & & \boldsymbol{\theta}_{t-1} & \rightarrow & \boldsymbol{\theta}_t & \rightarrow & \boldsymbol{\theta}_{t+1} & \text{intelligence} \\
 & & \uparrow & & \uparrow & & \uparrow & \\
\text{Switching Proc} & & W_{t-1} & \rightarrow & W_t & \rightarrow & W_{t+1} & \omega\text{'s position}
\end{array}
$$

$$
\begin{array}{lccccccccc}
\text{Intensity} & Z_{1t} & & Z_{2t} & & Z_{3t} & & Z_{4t} & & Z_{5t} \\
 & \uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
\text{Tasks} & \theta_{1t} & & \theta_{2t} & & \theta_{3t} & & \theta_{4t} & & \theta_{4t} \\
 & & \nwarrow & \uparrow & \nearrow & \uparrow & \nearrow & \uparrow & \nearrow & \\
\boldsymbol{\theta}_{I(w)} & & & \boldsymbol{\theta}_{I(w_1),t} & & \boldsymbol{\theta}_{I(w_1),t} & & \boldsymbol{\theta}_{I(w_3),t} & & \\
 & & & \uparrow & & \uparrow & & \uparrow & & \\
\text{RDCEG} & & & w_1 & \rightleftarrows & w_2 & \leftrightarrows & w_3 & &
\end{array}
$$

A Generic Explainable Bayesian Dynamic Model

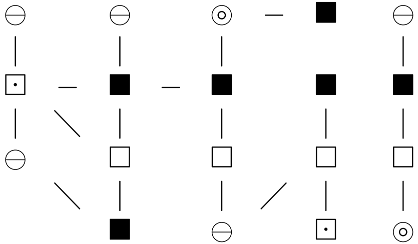
- **Suspect latent status** RDCEG: Condition model on this latent Markov process: joint dist. on time inhomogeneous parameter vectors of positions & transition parameters. **INTELLIGENT**
- **Tasks** $\boldsymbol{\theta}_{I(w_i),t}$ subvector of $\boldsymbol{\theta}_t$ - $p(\boldsymbol{\theta}_{I(w_i),t}|w_i)$ elicited through expert judgments. $p_\omega(\boldsymbol{\theta}_{I(w_i),t}|w_i)$ customised to ω via covariates + intelligence. DSS designed to adapt to new direct intelligence reports about tasks engaged in by ω. **INTERACTIVE OPEN MODEL**
- **Intensities** measure ω's activities z_{it} at time t for each task $\theta_{i,t}$: density $p(\mathbf{z}_t|\boldsymbol{\theta}_t)$. Often informed by open source data on innocent engagement tasks. **AGILE & ADAPTIVE**

$\boxed{\textbf{Technically} \text{ - Bayesian model fully specified!!}}$

$\Rightarrow$ ω's predicted threat levels $p_{\omega\tau}(w|\mathbf{z}^{(t)})$ at times $\tau \geq t$ automatically calculated in real time by DSS! (Bunnin & S, 21)

Graph: single attackers to gangs (Shenvi et al,22)

- Time slice **vertices** label each POI expected threat levels - $\boxdot, \square, \blacksquare$ benign $\ominus$, unknown $\circledcirc$ inherited from Bunnin &S(21).
- **Edges** $\Longrightarrow$ family/social, coconvictions, affiliates, in contact.
- Modify Chen et al (18): edges annotated dynamically updated **strengths** using discounted gamma - Poisson processes.



Even ignoring annotations **graph above not UG model** + **Vertex set dynamic** as POI's come & go. However has fully formal semantic $\Rightarrow$ represents a dynamic Bayesian model (Shenvi et al, 22). **Bespoke!!!**

Scoring the potentially most dangerous gangs

- **Threat scores** of potential gangs informed by coupling communication models with individual models.
- Choose score depending on **nature of threat**, what is known about **MO of potential attackers**, available **methods of frustrating** the attack, ... Often secure information!
- Scores typically a function of **group**, composite **capability**, **connectivity** of set (via edge weightings) & its **cohesiveness**.
- Most threatening groups = ones with highest scores highlighted ⇒ useful real time dashboards for operatives.
- ⇒ **scores explainable** - logically constructed from synthesis of Bayes & understandable expert judgements: open interactive tool!

Examples of these score functions given in Shenvi et al,(22).

Some concluding remarks

- **Subjective Bayesian methodology** & paradigm THE most promising way to combine rich data & critical expert judgments in real time policing decision support.
- New classes of model developed above have quite **generic applications**!
- Possible to guide development of appropriate **Bayesian modelling from behind a firewall**. Initially build models using only open source information & data $\longrightarrow$ coding this up $\longrightarrow$ transfer to police who customise their own parallel version of code inhouse embedding secure information $\longrightarrow$ academics calibrate inhouse code using disguised communications **Watch this space!!!**

Thank you for your attention!!!!!!!!!!!

Selected Publications by authors

Shenvi, A (21) "Dynamic Bayesian graphical models with public health & policing applications"PhD Thesis April 2021 Uni. Warwick
Bunnin, FO & Smith, JQ (21) "A Bayesian Hierarchical Model for Criminal Investigations" Bayesian Analysis :arXiv:1907.01894
Shenvi, A, Bunnin, FO & Smith, JQ (22) "A Bayesian decision support system for counteracting activities of terrorist groups"(accepted subject to revisions JSSA).
Wilkerson, RL& Smith, JQ (21) "Customised Structural Elicitation" ,In Expert Judgement in Risk & Decision Analysis Eds. Bedford T.et al,Springer p 83 -114
Smith JQ & Shenvi, A. (18) "Assault Crime Dynamic Chain Event Graphs" Warwick Wrap
Collazo, RA, Gorgen,C & Smith, JQ(18) "Chain Event Graphs" Chapman & Hall
Chen,K et al(18) "Scalable Bayesian modeling,monitoring & analysis of dynamic flow data" JASA,113,519-33
Smith,J.Q.(10) "Bayesian Decision Analysis: Principles & Practice" CUP

Performing secure technology transfer

contact + open source info. + elicitations + simulated use cases
$\downarrow$
1 Prototype Dynamic Probability Model $\longrightarrow$
documented Python code + user manual + Suite stats. diagnostics

....

$\Downarrow$
Parallel Inhouse Team (PIT) learns functionality of 1 $\rightarrow$
2 PIT write own parallel inhouse code embedding secure structural info.
$\rightarrow$
PIT tests against own secure data sets & secure case studies $\rightarrow$
PIT analogue system discovers inadequacies in algorithms.

....

$\Downarrow$
Secure communication $\rightarrow$ Turing team recodes $\rightarrow$ 1 $\uparrow$
$\circlearrowleft$ Repeat until PIT system fit for purpose.

Task Integrity: A customised assumption within hierarchy

Updating position probs when tasks directly observed. Specify relative to innocent!

Task set integrity demands $I^*(w_i)$ is defined so that for all $i = 1, 2, \ldots, m$, $0 \leq t \leq T$,

$$W_t \amalg \boldsymbol{\theta}_t | W_t \in \{w_0, w_i\}, \boldsymbol{\theta}_{I^*(w_i),t}$$

Equivalent to equation

$$\frac{p_t\left(w_i|\boldsymbol{\theta}_t, \mathcal{F}_t\right)}{p_t\left(w_0|\boldsymbol{\theta}_t, \mathcal{F}_t\right)} = \frac{p_t\left(w_i|\boldsymbol{\theta}_{I^*(w_i)t}, \boldsymbol{\theta}_{\widehat{I}^*(w_i)t}, \mathcal{F}_t\right)}{p_t\left(w_0|\boldsymbol{\theta}_{I^*(w_i)t}, \boldsymbol{\theta}_{\widehat{I}^*(w_i)t}, \mathcal{F}_t\right)}$$

is a function only of $\boldsymbol{\theta}_{I^*(w_i)t}$ where $\widehat{I}^*(w)$ is set of indices $\notin I^*(w)$.

Notes If tasks chosen to discriminate position well:

1. Someone in position w_i will have prob. ≥ 0.2 of engaging in all tasks simultaneously.
2. OTOH an innocent will simultaneously engage often product of small terms ($\amalg$).