IMPERIAL

Clustering mutually-exciting Hawkes processes for honeypot sessions

Daniyar Ghani, Nick Heard, Francesco Sanna Passino

21 August 2025

Agenda

Motivation: honeypot sessions

- Computer terminal commands arrive on honeypot in sessions.
- Sessions made up of commands, tokenised into words.

```
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /
wget http://abc.def.ghi.jkl/Zerow.sh
curl -O http://abc.def.ghi.jkl/Zerow.sh
chmod 777 Zerow.sh
sh Zerow.sh
tftp abc.def.ghi.jkl -c get tZerow.sh
chmod 777 tZerow.sh
sh tZerow.sh
rm -rf Zerow.sh tZerow.sh
```

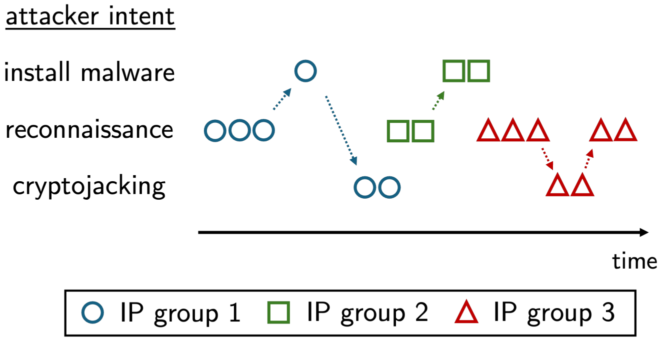
command

subcommand (word)

Example session

Motivation: clustering of sessions and IPs

- Sessions and commands can be grouped by attacker intent.
- Attacker behaviour evolves over time: investigate temporal dynamics.
- Sessions originate from multiple IP addresses.
- Useful to identify groups of coordinated/related threat actors.



Existing work

- Topic models cluster documents (sessions) by words (commands) only.
- Hawkes processes capture temporal self and mutual-excitation.

Authors	Model structure	Inference	Application
Li et al., 2014	Latent Dirichlet allocation (LDA) + self-exciting Hawkes	VI	Modelling search engine queries
He et al, 2015	Correlated topic model + mutually-exciting Hawkes	VI	Diffusion of information in text
Du et al., 2015	Dirichlet process mixture + self-exciting Hawkes	MCMC + SMC	Clustering document streams
Zheng et al, 2021	Dirichlet process + marked self-exciting Hawkes	SMC	Cyber threat detection via user activity modelling
Goda et al., 2022	LDA + mutually-exciting Hawkes	MLE	Propagation of ideas in social networks

Table: Examples of models combining topic models with Hawkes processes.

Topic–IP Point Process (TIPP) model

- Combines topic modelling with mutually-exciting point processes.
- Clusters sessions by attacker intent via constrained Bayesian clustering (CBC, Sanna Passino et al., 2025): single topic per session.
- Temporal dynamics modelled by multivariate Hawkes process (MHP).
- Cluster source IPs.

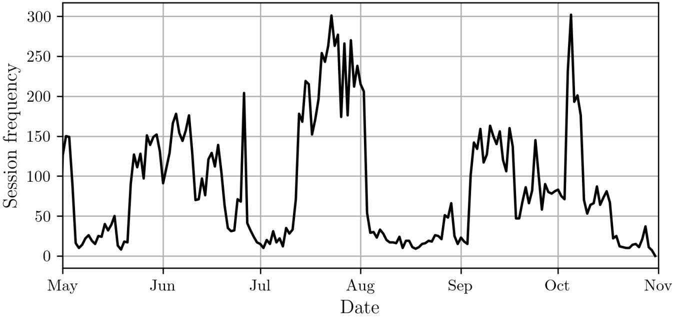
Topic–IP Point Process (TIPP) model

- Combines topic modelling with mutually-exciting point processes.
- Clusters sessions by attacker intent via constrained Bayesian clustering (CBC, Sanna Passino et al., 2025): single topic per session.
- **Temporal dynamics modelled by multivariate Hawkes process (MHP).**
- **Cluster source IPs.**

Focus: recovery of Hawkes parameters and IP groups.

Honeypot data

- Sessions collected between May and Nov 2023.
- Observe: timestamps t, source IP addresses y, commands w.
- Latent: topics z, IP groups γ.
- 15990 sessions over $U = 20$ IP addresses.



TIPP model: sessions

- Each session is (t_d, z_d, y_d, w_d) = (time (hours), topic, IP, commands).
- Latent topic z_d represents attacker intent.
  - *For now: assume topics are known, learned via topic model.*
- IP address y_d has group $\gamma(y_d)$.

Session	**Time** t	**Topic**	**IP** y	**IP group** $\gamma(y)$
nmap -sV 10.0.0...	0.5	reconnaissance	1XX.1XX.3X.2X	1
wget http://mal...	1.2	install malware	2XX.X.1XX.7X	2
./xmrig -o str...	2.8	cryptojacking	1XX.5X.1XX.4X	3

Table: Example honeypot session activity.

TIPP model: Hawkes process

- Sessions arrive via MHP with latent topic $z_d = k$ and source IP $y_d = u$.
- Conditional intensity for (k, u):

$$\lambda_{k,u}(t) = \lambda^0_{k,u} + \lambda^{(z)}_{k,u} + \lambda^{(y)}_{k,u} + \lambda^{(z,y)}_{k,u}$$

  - λ^0 : baseline intensity.
  - $\lambda^{(z)}$: mutual-excitation from topic k and IPs in group $\gamma(u)$ excluding u.
  - $\lambda^{(y)}$: mutual-excitation from IP u and topics active for group $\gamma(u)$ excluding k.
  - $\lambda^{(z,y)}$: self-excitation from topic k and IP u.

TIPP model: Hawkes process

- Sessions arrive via MHP with latent topic $z_d = k$ and source IP $y_d = u$.
- Conditional intensity for (k, u):

$$\lambda_{k,u}(t) = \lambda^0_{k,u} + \lambda^{(z)}_{k,u} + \lambda^{(y)}_{k,u} + \lambda^{(z,y)}_{k,u}$$

  - λ^0 : baseline intensity.
  - $\lambda^{(z)}$: mutual-excitation from topic k and IPs in group $\gamma(u)$ excluding u.
  - $\lambda^{(y)}$: mutual-excitation from IP u and topics active for group $\gamma(u)$ excluding k.
  - $\lambda^{(z,y)}$: self-excitation from topic k and IP u.
- **Self-excitation: observing (k, u) makes (k, u) more likely.**
- **Mutual-excitation: observing (k, u) makes *related* (k', u') more likely.**

TIPP model: excitation kernels

- Intensities:

$$\lambda_{k,u}(t) = \sum_{\substack{t_i < t \\ (z_i, y_i) = (k,u)}} \omega_{k,u}(t - t_i)$$

- Excitation kernels take scaled exponential forms:

$$\omega_{k,u}(t - t_i) = \rho_{k,u} \exp\{-(\rho_{k,u} + \sigma_{k,u})(t - t_i)\}$$

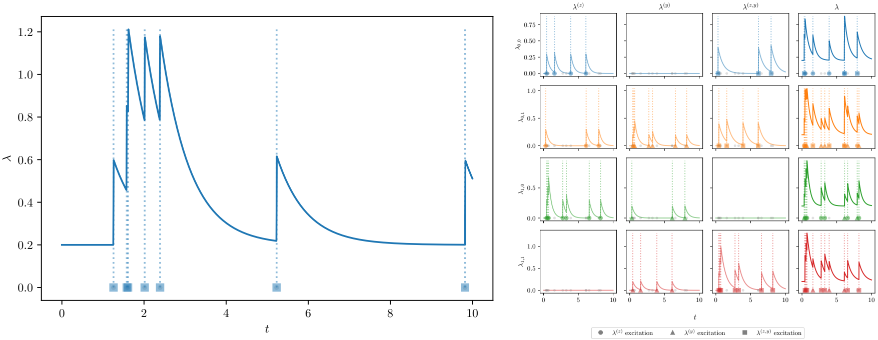
- Enables fast computation of Hawkes likelihood (Daley & Vere-Jones, 2003):

$$L(T) = \prod_{k,u} \left[\prod_{j=1}^{N_{k,u}} \lambda_{k,u}(t_{k,u}^{(j)}) \right] \exp\{-\Lambda_{k,u}(T)\}$$

where $\Lambda_{k,u}(t)$ is the compensator for process (k, u).

Simulations

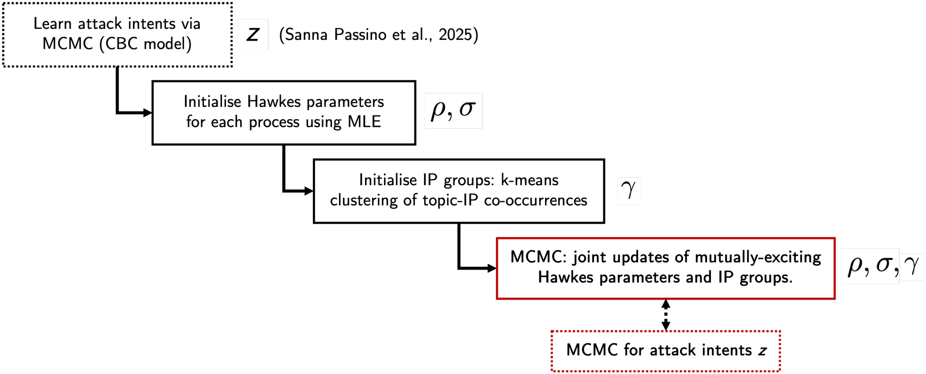
- Simulate Hawkes process: adaptation of Ogata, 1981 and Chen, 2016.
- Univariate: jump $\rho = 0.2$, "decay" $\sigma = 2.0$.
- Multivariate: self and mutual-excitation.



Simulated intensities (left: univariate, right: multivariate)

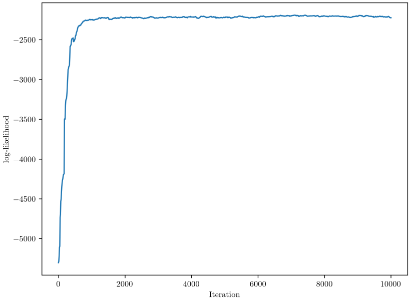
Inference framework

1. Infer session topics z using CBC via MCMC (Sanna Passino et al., 2025).
2. Fit Hawkes parameters ρ, σ and IP groups γ conditional on topics.
3. Optional: update z conditional on ρ, σ, γ.



Application to honeypot data

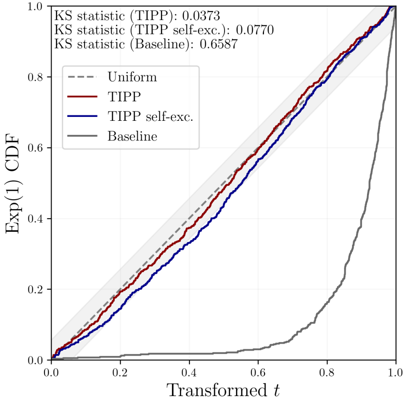
- CBC assigns $K = 5$ topics.
- MCMC: 10,000 iterations.



Likelihood trace

Model fit diagnostics

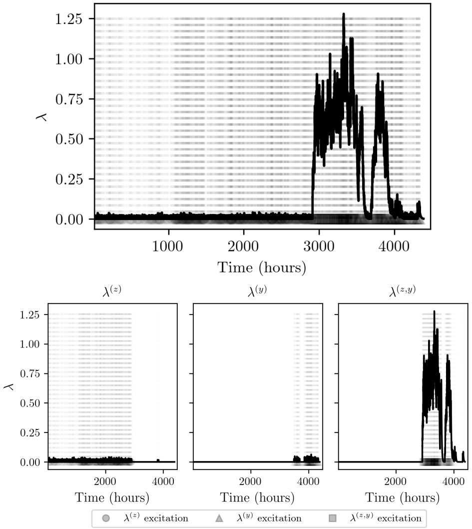
- Residual analysis and KS test for goodness-of-fit.
- TIPP outperforms baseline and self-exciting-only processes.



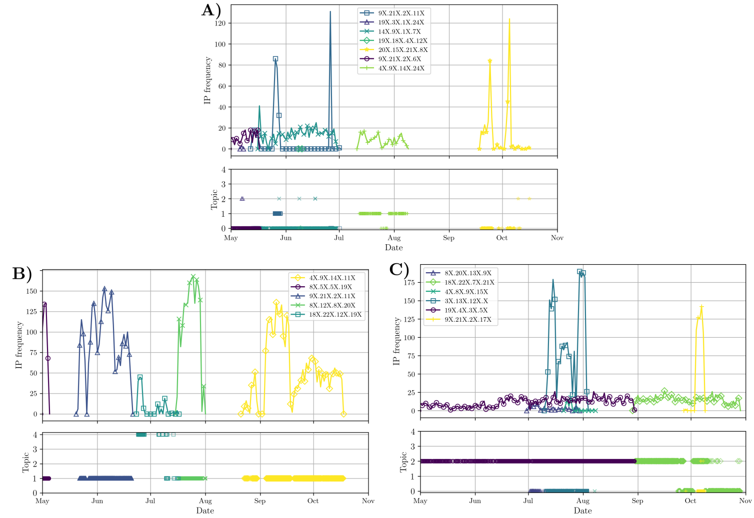
KS residual plot

Fitted intensities

- Some mutual-excitation, but intensities dominated by self-excitation.



IP grouping



Topic-IP frequencies

Conclusion

- Integrated topic models with Hawkes processes.
- Additional features (time, source IP) are useful for honeypot session analysis.
- **Can identify coordinated threat actors via IP grouping.**
- Future ideas: filter automated sessions, scalability, change-point detection.

IMPERIAL

Thank you!
Questions?