Sandia National Laboratories

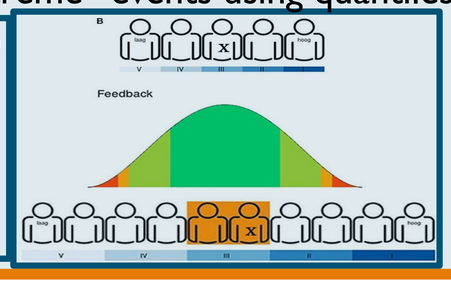
SEQUANA: SEQUential ANomaly Analysis

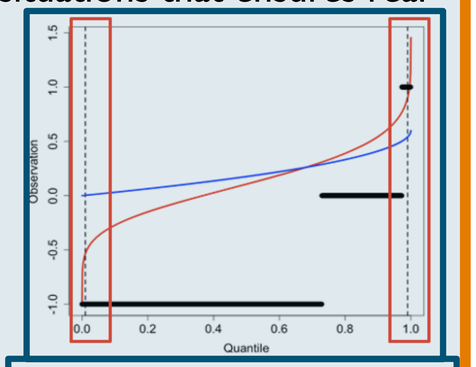
Lekha Patel (PI), Doug McGeehan, Gabriel Huerta, Peter Jacobs, Mayuri Shakamuri, Miguel Palaviccini, Fletcher Christensen (UNM)

Significance & Goals

- Sequana is a novel statistical and computational capability intended to quantify high impact, rare and unanticipated situations that ensures real-time responses to extreme events.
- Sequana provides a flexible **unsupervised** statistical framework to quantify anomalies.
- Will **quantify real-time probabilities** of observing "extreme" events using quantiles.

Expert elicitation to be deployed to fully characterize SEQUANA for specific applications.

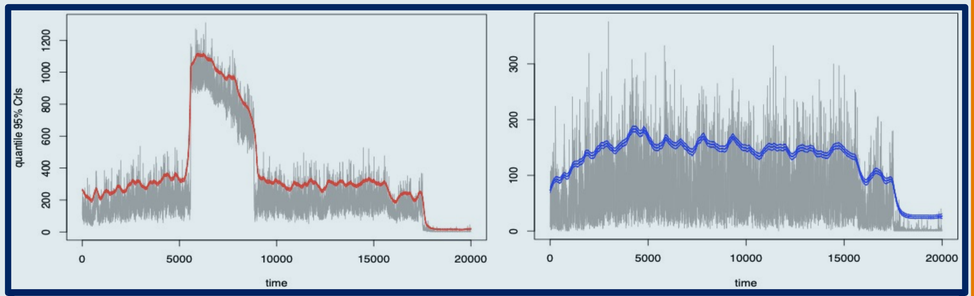




Different forms of quantile functions accompanied by values attained beyond the lower 5% and upper 95% quantiles.

Statistical learning approach

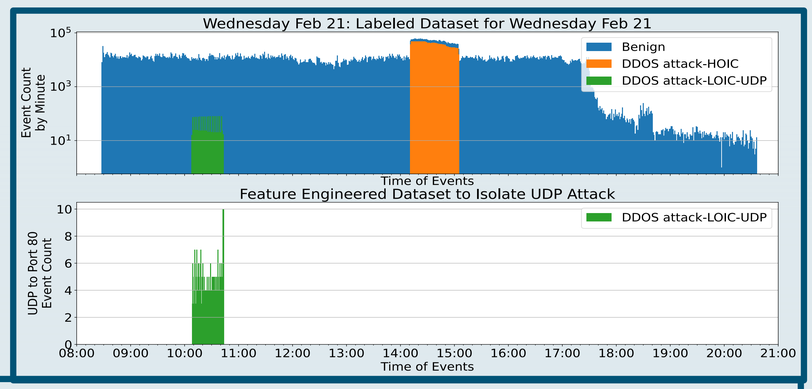
- Propagate unknown quantile function, which is less influenced by extreme values via state-space modeling.
- **Variational Bayesian Kalman-style** prediction and updating of quantile function, leads to risk characterization over all quantiles.
- Application unique parameter specifications via expert elicitation **to determine anomalies.**



Single quantile anomaly classification (left) vs fixed quantile limitations to anomaly detection (right) in cyber-security,

Cybersecurity exemplar

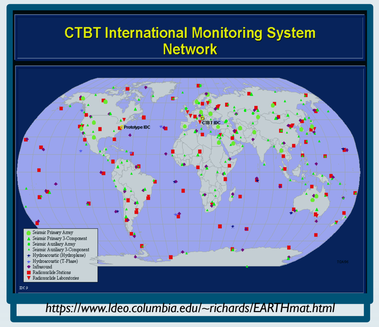
- Sequana will quantify computer network traffic anomalies in a streaming fashion from historic data.
- Developed **novel feature-engineering techniques** enable data to contain more events and complex features than raw data.



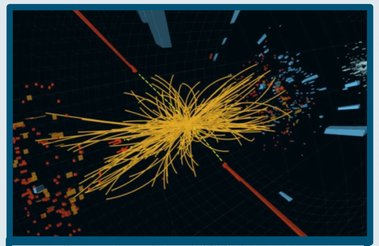
Aggregated events from a computer network over time. Specific aggregations and events require expert elicitation to then be used for anomaly *classification.*

Impacts & Successes

- Sequana is to be generalized to target anomalies from a wide range of applications.
- Future impact to other mission spaces e.g. detecting anomalous pathogens, nuclear seismic monitoring from remotely sensed data, weapons' product testing or new particle physics detection, beyond studied exemplars.
- Conference presentation accepted at the international conference on Bayesian Nonparametrics (ISBA) in October 2022.
- Preparing manuscript "Feature engineering for cyber-security event data" for submission to the Journal of Machine Learning Research.



https://www.ldeo.columbia.edu/~richards/EARTHmat.html



https://arstechnica.com/science/2019/07/mit-physicists-social-networks-could-hold-the-key-to-finding-new-particles/

Funded by the National Security Information Sciences and Technology (NSIST) LDRD program **(Year 1/3)**; FTE: 1.2.