MACB: Machine Learning Based Anomaly Detection in 1553 Bus Commands Behavior Manipulation

Dr. Mohammad Mozumdar

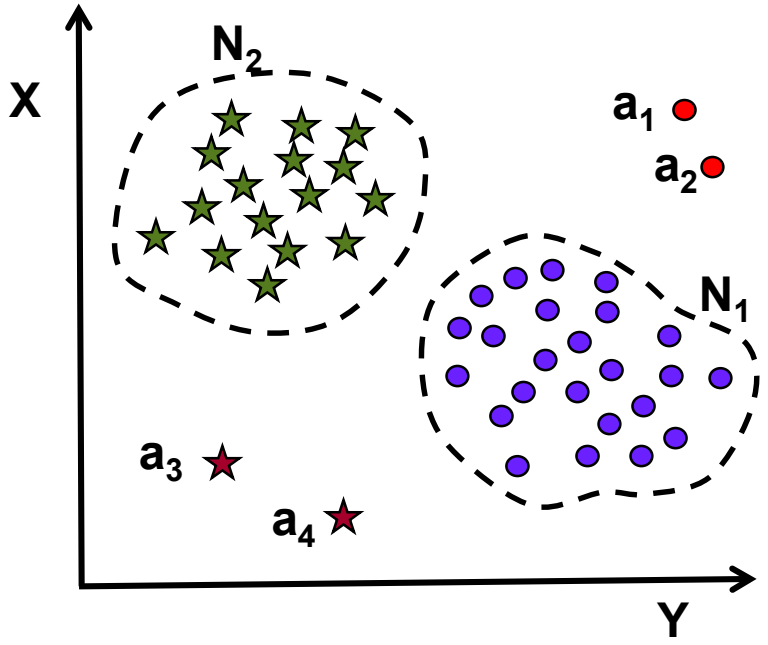
Information Systems & Cyber Division
The Aerospace Corporation

What are Anomalies?

- Anomalies are ***patterns*** in data that do not conform to a well defined notion of normal behavior.

- ***N_1*** and ***N_2*** contains data points in normal behavior regions.

- Data points ***a_{1-4}*** are anomalies!



- Anomaly detection is related to, but distinct from ***noise removal*** and ***noise accommodation***, both of which deal with unwanted noise in the data.

Anomaly Detection and Challenges

- A straightforward anomaly detection approach could be to define a ***region representing normal behavior*** and declare any observation in the data that ***does not belong*** to this ***normal region*** as an ***anomaly***. **However…**

  – *Defining a **"normal"** region that encompasses **every possible normal behavior is very difficult**.*

  – **Boundary** between ***normal and anomalous behavior*** is often ***not precise***.

  – When anomalies are the result of malicious actions, the malicious adversaries often adapt themselves to make the ***anomalous observations appear normal*****.**

Type of Anomalies

Anomalies can be classified into following ***three categories***:

- **Point Anomalies:** If **an individual data instance** can be considered as anomalous with respect to the rest of data, then the instance is termed a point anomaly

- **Contextual Anomalies:** If a data instance is anomalous in a **specific context**, but not otherwise, then it is termed a contextual anomaly

- **Collective Anomalies:** If a **collection of related data** instances is anomalous with respect to the entire data set, it is termed a collective anomaly

Supervised VS Semi-supervised VS Unsupervised Anomaly Detection

- **Supervised Anomaly Detection:** Techniques trained in supervised mode assume the availability of a training data set that has **labeled instances** for **normal** as well as **anomaly** classes.

- **Semi-supervised Anomaly Detection:** Techniques that operate in a semi-supervised mode, assume that the **training data** has **labeled** instances **only** for the **normal** class.

- **Unsupervised Anomaly Detection:** Techniques that operate in unsupervised mode **do not require labeled training data**.

Need for anomaly detector for 1553 Bus

- Globally distributed supply chain for system development
  - *Supply chain attack -> malicious code injection*
- Detect new hardware or software
- New behavior analysis of updated system
- Diagnostics of system flaws

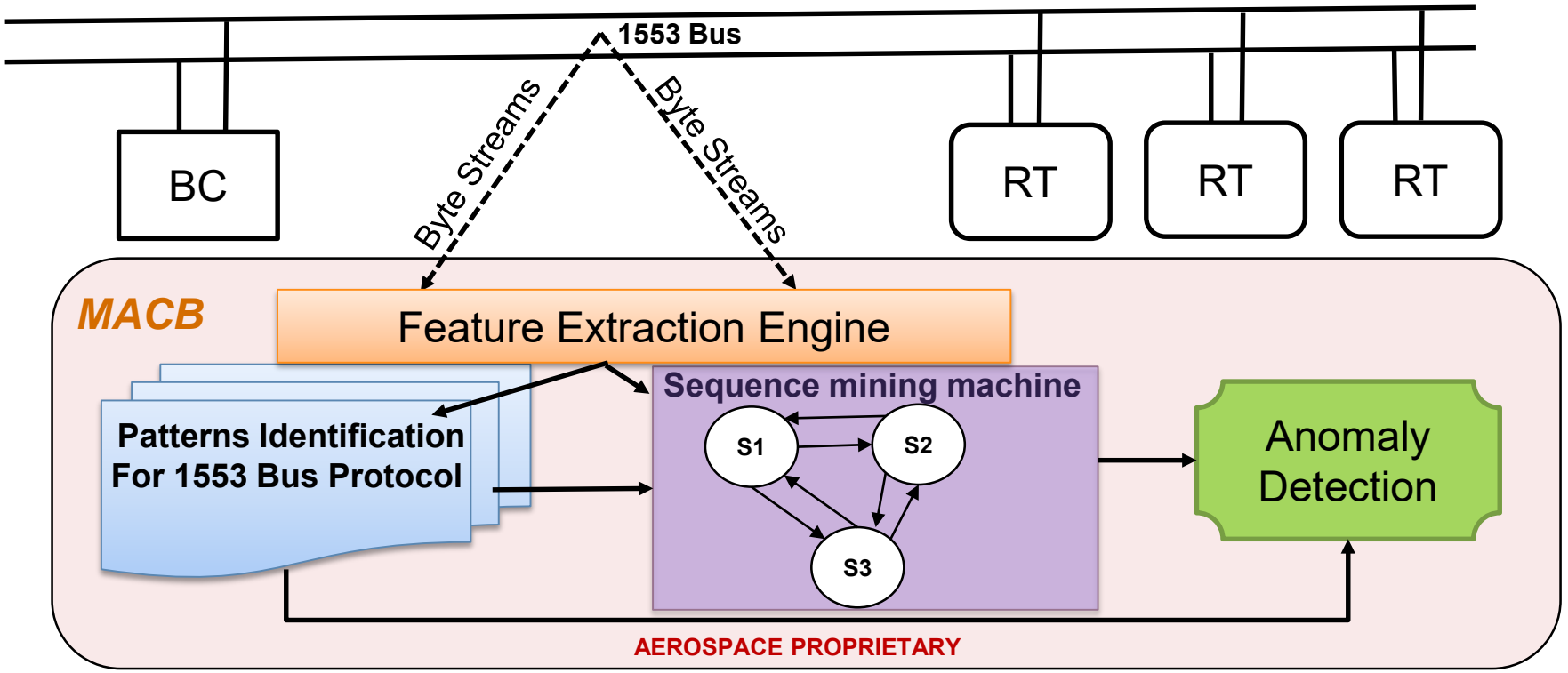
- The type of solution required
  - Anomaly detection method independent of 1553 protocol implementation
  - Lightweight, highly flexible and adaptable

Aerospace solution is MACB!

MACB: *M*achine Learning Based *A*nomaly Detection for 1553 Bus *C*ommand Word *B*ehavior Manipulation

- *MACB* **constructs** *BUS commands* ***sequence*** from the byte streams **automatically**, hence MACB doesn't require to know the bus communications protocols beforehand.

- *MACB* uses sequence mining algorithm that derives a model representing valid transitions of commands from non-anomalous command streams.



** Patent submission in process by The Aerospace Corporation **

Problem Formulation: Point Anomaly in 1553 Bus Command

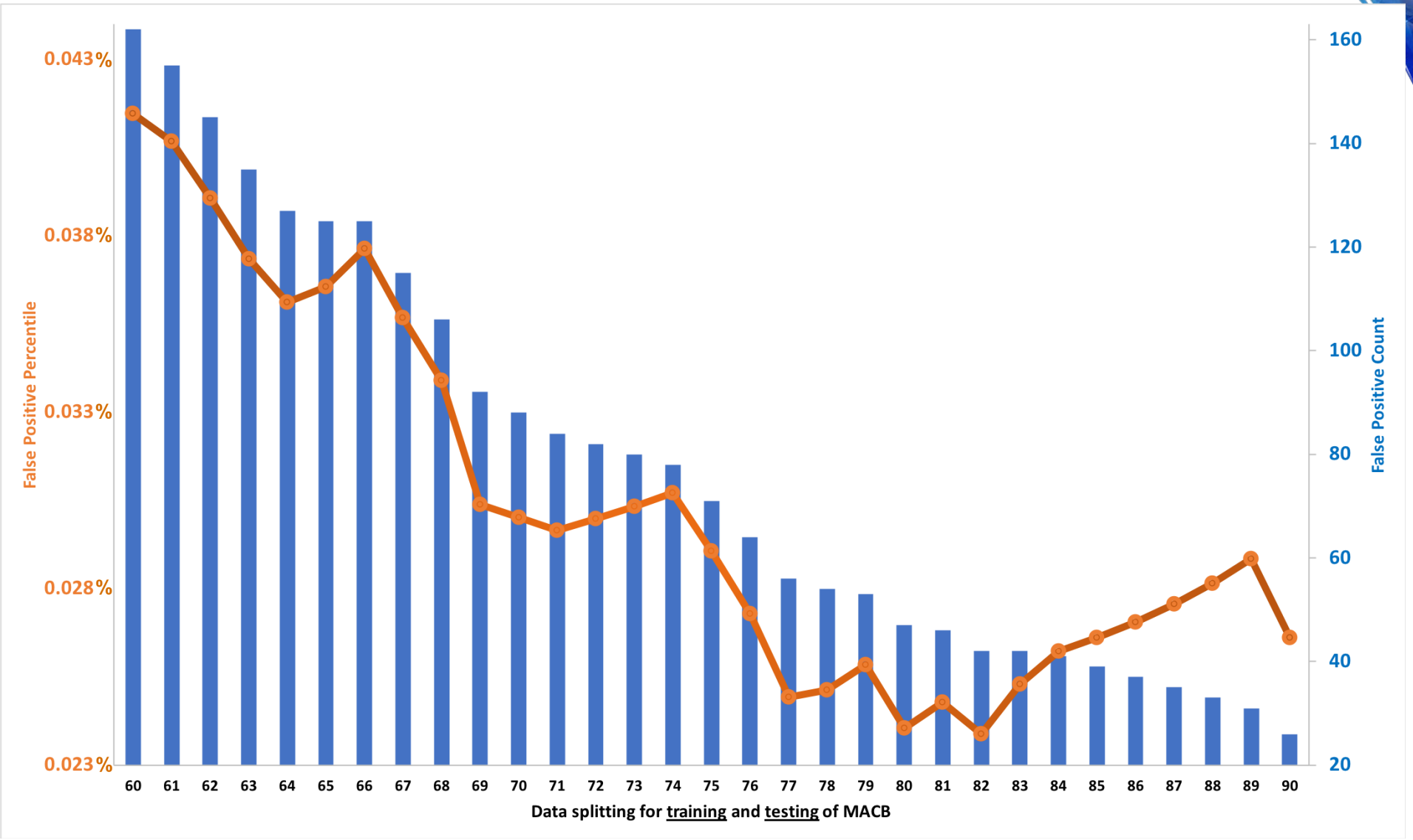
1821|3433|2422|1821|2021|2021||3841|3041|1821|1821|3c2e|3433|1821|2422|2021|2021||3041|1821|3433|2021|2021|2422||1821|3c2e|1821|3433|1821|2422|2021|2021||1821|1821|1821|3c2e|3433|2422|2021|2021||1821|1821|3c2e|3433|1821|2021|2021|2422||1821|1821|1821|3c2e|2021|2021|3433|...**Couple of thousands....** .2422|1821|3433|2422|1821|2021|2021||3841|3041|1821|1821|3c2e|3433|1821|2422|2021|2021||3041|1821|3433|2021|2021|2422||1821|3c2e|1821|3433|1821|2422|2021|2021||1821|1821|1821|3c2e|3433|2422|2021|2021||1821|1821|3c2e|3433|1821|2021|2021|2422||1821|1821|

|3841|3041|3c2e|1821|3433|2422|1821|1821|2021|2021||3841|3041|1821|3c2e|1821|3433|2422|1821|2021|2021||3841|3041|1821|1821|3c2e|3433|1821|2422|2021|2021||3041|1821|1821|1821|2021|2021|3c2e|3433||1821|1821|1821|2021|2021|3c2e|3433|2422||1821|3c2e|3433|2422|1821|1821|2021|2021||1821|3c2e|3433|1821|2422|1821|2021|2021||3c2e|3433|1821|2422|1821|1821|2021|2021||1821|1821|3c2e|3433|**3c2e**|1821|2021|2021||3c2e|3433|1821|1821|2422|1821|2021|2021||1821|1821|3c2e|1821|3433|2422|2021|2021||1821|1821|1821|3c2e|3433|2021|2021|2422||1821|3c2e|1821|3433|1821|2422|2021|2021||1821|1821|1821|3c2e|3433|2422|2021|2021||1821|1821|3c2e|3433|1821|2021|2021|2422||1821|1821|1821|3c2e|2021|2021|3433|2422|

1821|3433|2422|1821|2021|2021||3841|3041|1821|1821|3c2e|3433|1821|2422|2021|2021||3041|1821|3433|2021|2021|2422||1821|3c2e|1821|3433|1821|2422|2021|2021||1821|1821|1821|3c2e|3433|2422|2021|2021||1821|1821|3c2e|3433|1821|2021|2021|2422||1821|1821|1821|3c2e|2021|2021|3433|...**Couple of thousands....** .2422|1821|3433|2422|1821|2021|2021||3841|3041|1821|1821|3c2e|3433|1821|2422|2021|2021||3041|1821|3433|2021|2021|2422||1821|3c2e|1821|3433|1821|2422|2021|2021||1821|1821|1821|3c2e|3433|2422|2021|2021||1821|1821|3c2e|3433|1821|2021|2021|2422||1821|1821|

Possible 1553 Bus commands: 0x1821, 0x2021, 0x2422, 0x3433, 0x3041, 0x3c2e, 0x384

Anomaly Detection - False Alarm Rate (False positive)



Thanks!