Immunising Automated Teller Machines

Jon Timmis

Rogerio De Lemos

Modupe Ayara

Simon Forrest

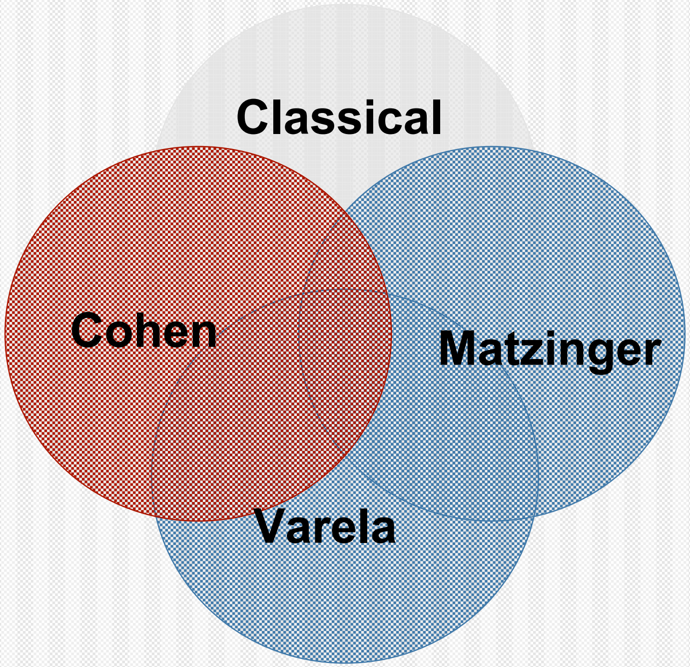
Background

- Industrial based research
- Dependability of embedded systems
  - Focus on *availability* of an ATM.
  - ATMs are expensive to repair and cost of ownership increases if they are out of action
- Fault tolerance is a means to improved availability
  - *error detection*
  - recovery

Adaptable error detection as a means to improved availability

- Error detection
  - Improved error detection enhances availability
  - Error detection techniques usually exploit known systems profile for detecting error states and behaviour
  - These error detection techniques are limited to the detection of errors known at design-time of systems
  - *Adaptable error detection* is aimed at detecting errors that were not known during the design-time of systems

What is the Immune System ?



- The are many different viewpoints
- These views are not mutually exclusive
- Lots of common ingredients

From a computational perspective:

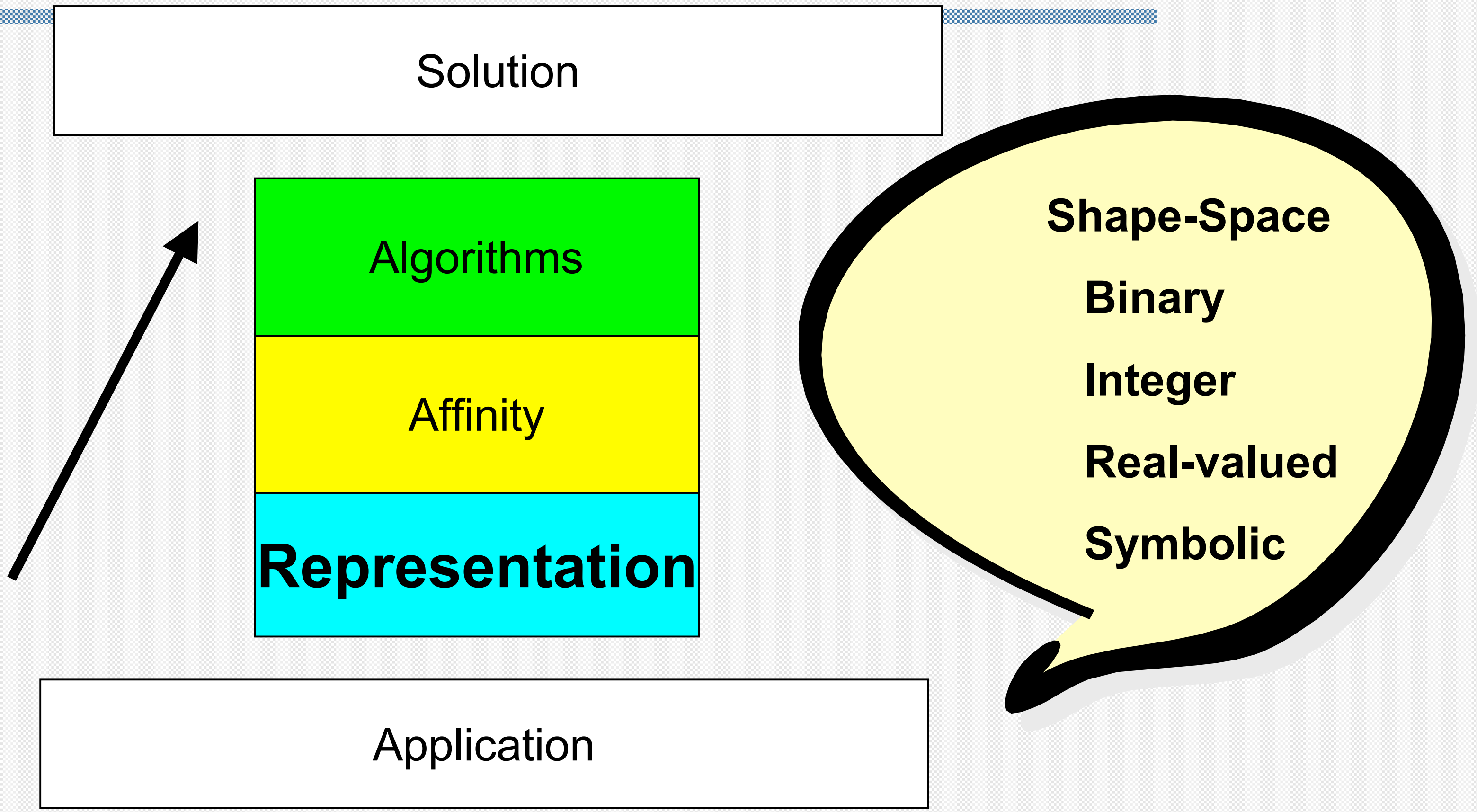
Computational Properties

- Unique to individuals
- Distributed
- Imperfect Detection
- Anomaly Detection
- Learning/Adaptation
- Memory
- Feature Extraction
- Diverse
- ..and more

Systems that are:

- Robust
- Scalable
- Flexible
- Exhibit graceful degradation
- Homeostatic

A Framework for AIS

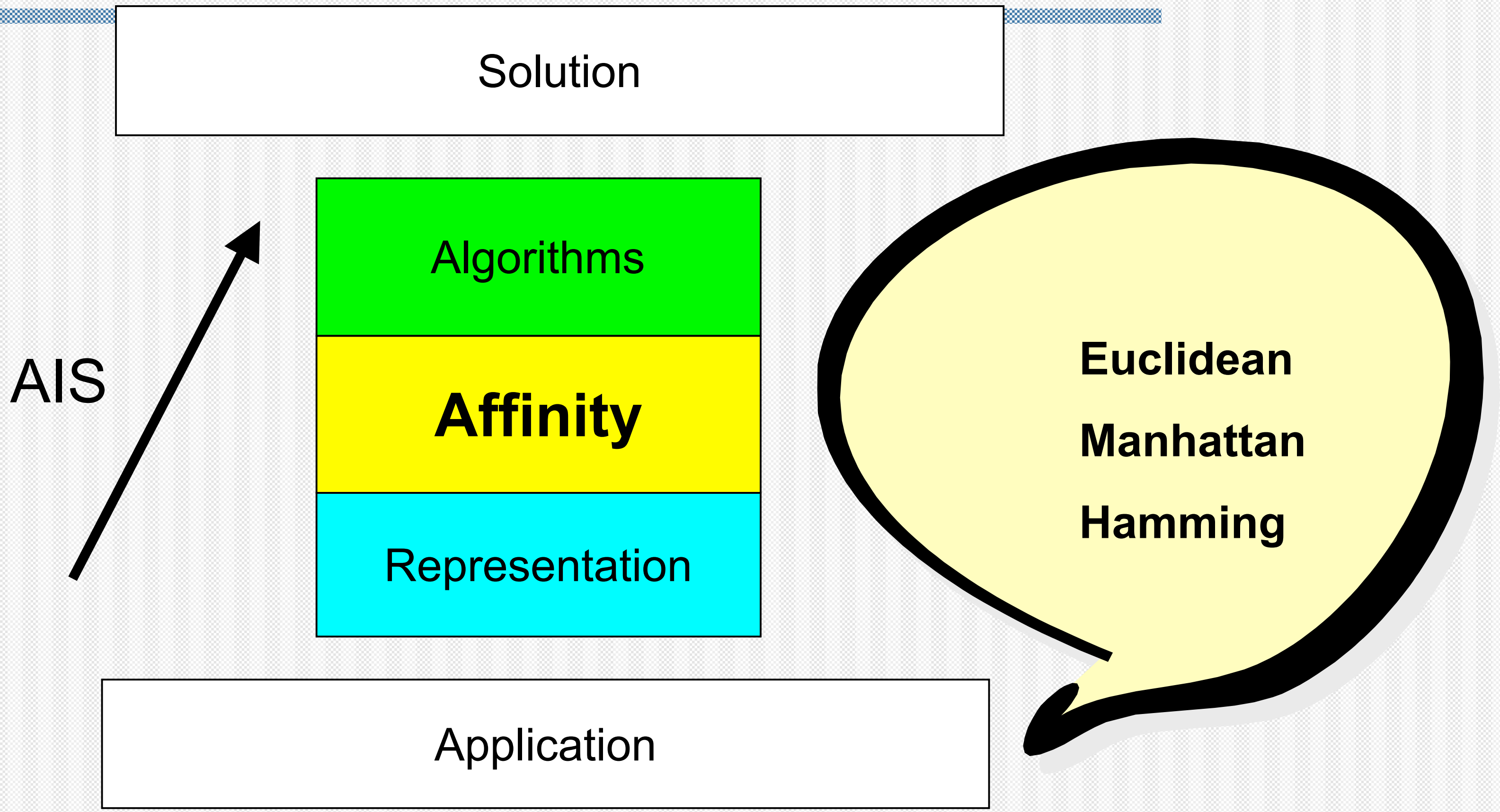


[De Castro and Timmis, 2002]

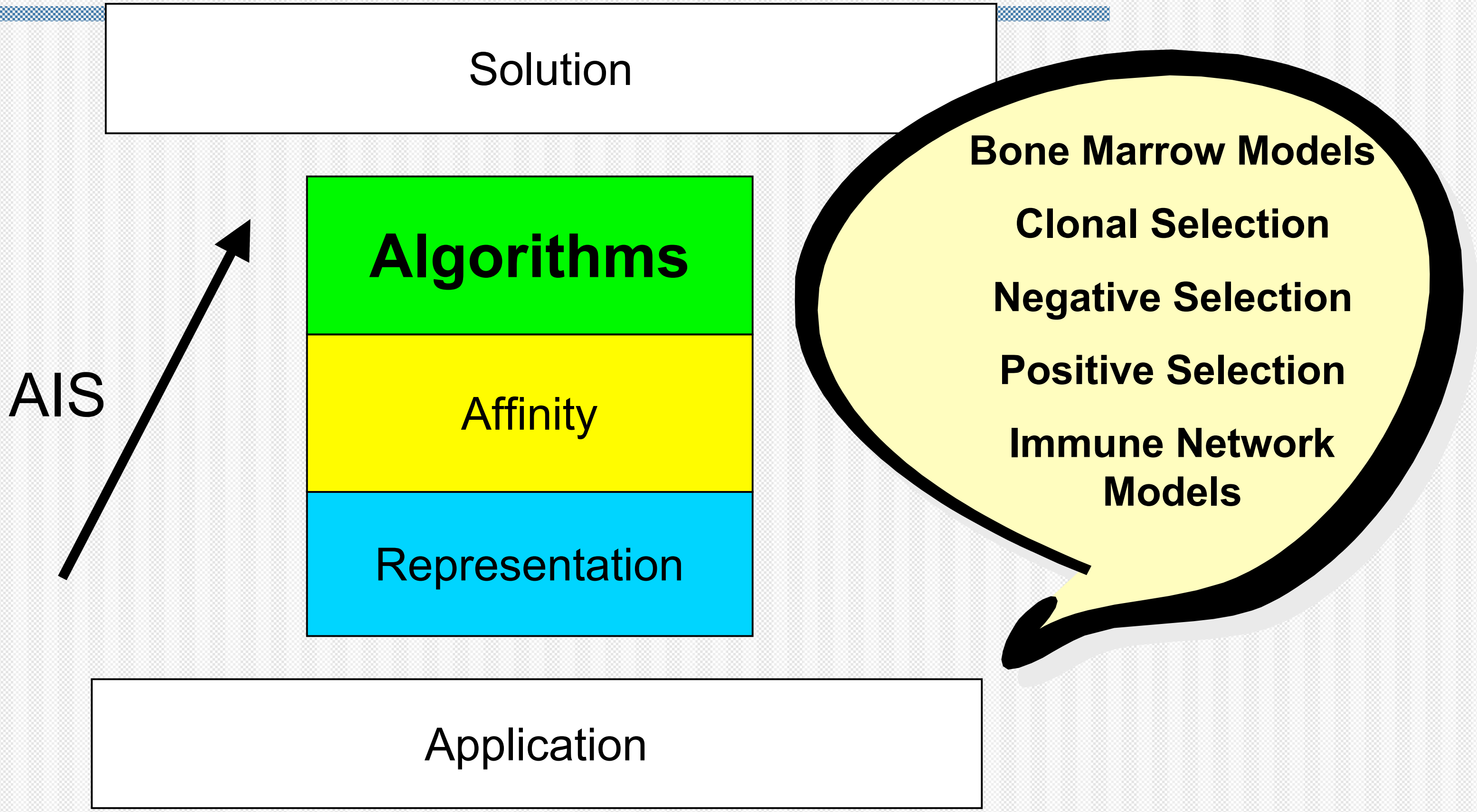
AIS

THE UNIVERSITY of York

A Framework for AIS



A Framework for AIS



AIS for fault tolerance

- Motivation for immune-inspired fault tolerance (Avizienis, 1997)
- Software fault tolerance (Xanthkis et al., 1996)
- Hardware fault tolerance
  - Fault diagnosis (Ishida, 1997)
  - Error detection (Bradley and Tyrrell, 2000)

Challenges then for Immune Inspired Fault Tolerance

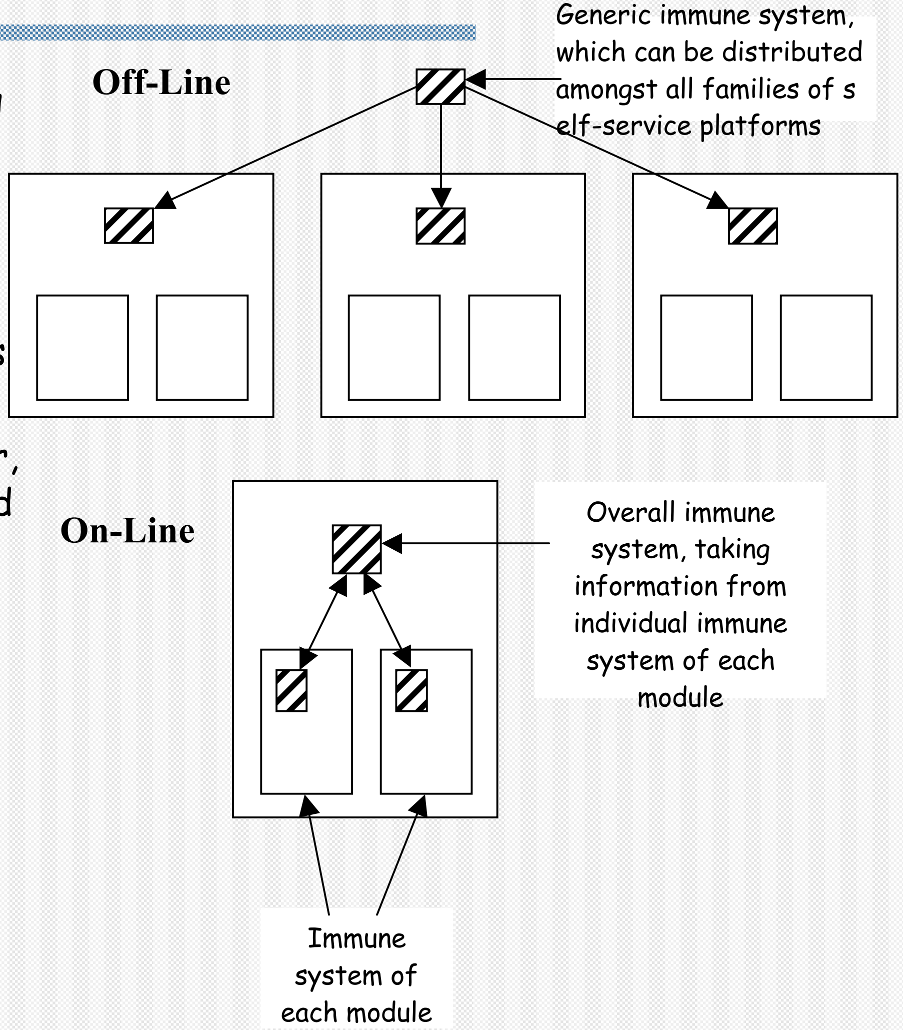
- Data representation
  - We settled on M-status
- Minimal number of detectors
  - Have notion of generalised detectors
- Coping with change in the system
  - Require a system that can learn new failures and adapt to create a specific immune system for each ATM
    - Then **immunise other machines**!

Outline of the System (Patent for self-service platforms)

- ATMs are able to learn their corresponding pattern of usage, which is used for future predictions and recommendations for maintenance.

- ATMs can notice gradual undesired changes to performance of the system
  - trigger alerts to system's behaviour, and provide corresponding degraded services as a consequence of undesired changes.
- The system can be distributed amongst different families of ATMs.

- Novel undesired changes learnt by local immune system can be distributed to other ATMs.



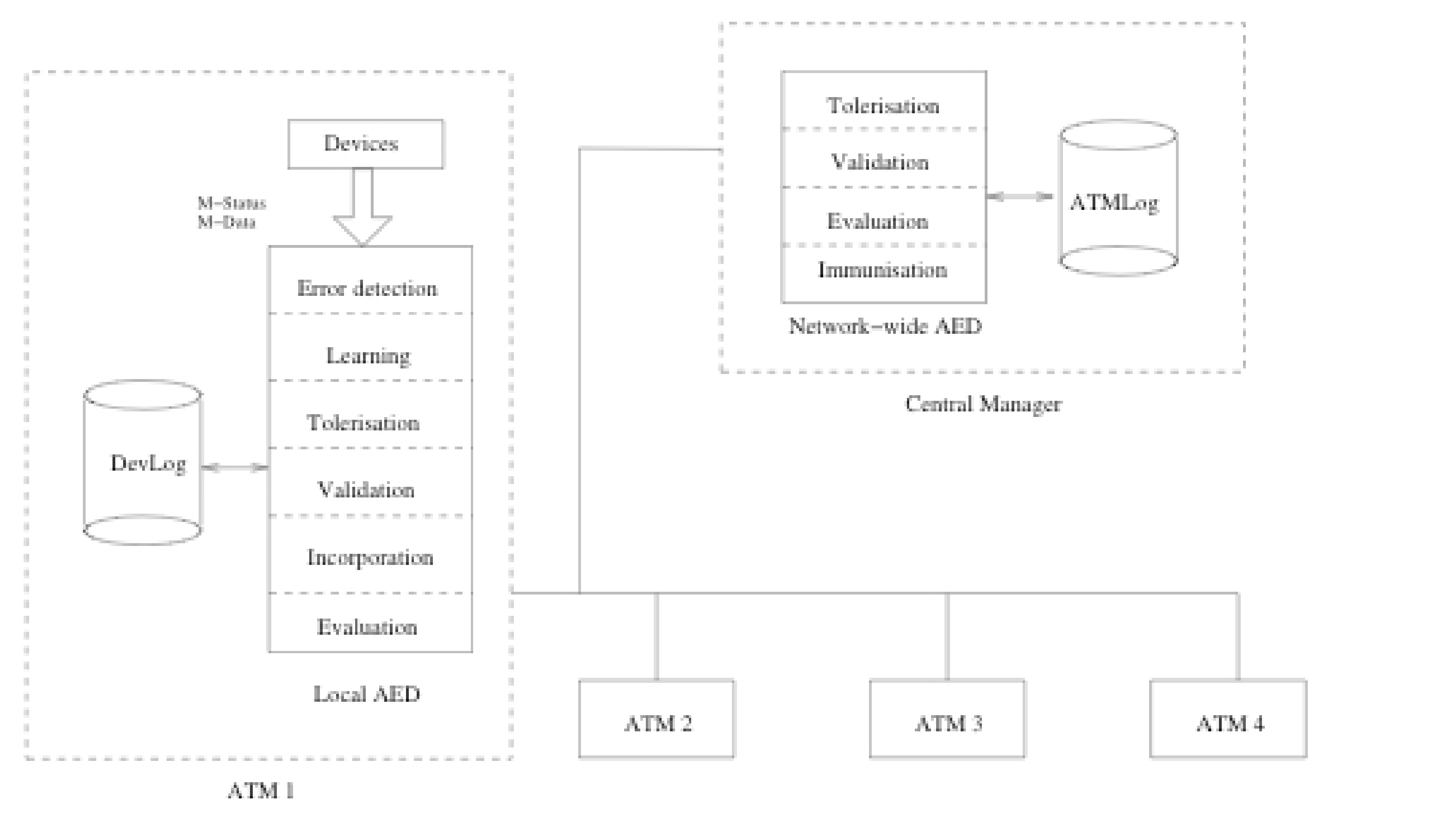
Features of the patent

- Differences between our system and prior designs:
  - The system is able to learn changes to normal states and behaviours of the ATM and incorporate into its knowledge;
  - The system can learn new erroneous behaviours and generate corresponding detectors;
  - The system can be distributed amongst different families of self service platforms;

Framework for adaptable error detection

- Immune-inspired
  - Vaccination
  - Continual learning
- Two-phases
  - Design-time immunisation
  - Run-time adaptation
- Two levels
  - Local AED
  - Network-wide AED

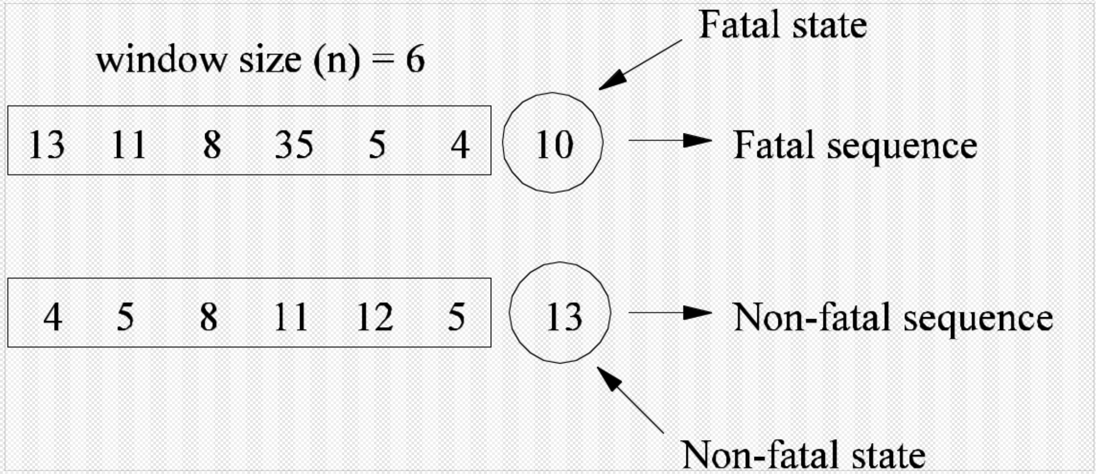
Architecture for Adaptable error detection (AED) in ATMs



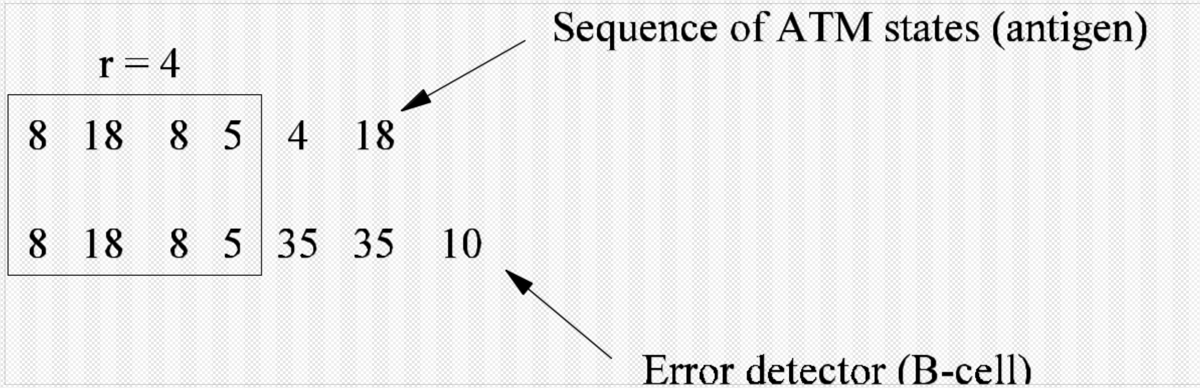
Artificial immune system for implementing local AED in ATMs

The University of York

Representation



Affinity Measure



$$\text{Affinity} = \frac{\text{contiguous states}}{\text{window size} + \text{abs}(\text{B-cell-Interval} - \text{Antigen-Interval})}$$

Algorithm and Processes

- Dynamic clonal selection
  - Mutation via evolved gene libraries
  - Mutation via the incorporation of fatal sequences
- Criteria for evaluation
  - Classification accuracy, true positive, false positive, true negative, false negative rates (classification performance)
  - Mean detection time interval

AISEC (dynamic clonal selection)

- Representation of one data class
  - B cells represent failure sequences
- Gene Libraries
  - Libraries of sequences of states (legal) used in mutation to create a new B cell
- Cloning
  - Random clones are not produced (make meaningless B cells)

AISEC

- Co-stimulation
  - A B cell classifies a sequence as a potential failure. They are moved to a temp. store. B Cell rewarded if a successful classification (validated by engineer)
- Cell death
  - If B cells does not stay stimulated, it dies.

Experimental results: Classification Accuracy

	Data set A	Data Set B
Accuracy	92.98(1.74)	89.85(.21)
TP	88.89(2.75)	57.5 (1.5)
TN	98.61 (.10)	98.61(.10)
FP	1.98 (0.10)	1.39 (.10)
FN	11.11(2.75)	43.5 (1.5)

Mean Detection Time

	Data set A	Data set B
Mean detection time	2:25:10 (0:5:20)	11:21:22 (0:3:35)

Conclusions

- Prototype detects fatal sequences prior to the occurrences of failures
  - Enhancement of availability in ATMs
  - Limited set of data, but there does seem to be a trade off between MTF and confidence
- Continuous learning improves the classification accuracy of the prototype
- Useful, as NCR have patented the idea and are incorporating some of the ideas into systems
- Demonstrated the potential, and is seen as one aspect of our new work on fraud (and fault) detection