A Data-Driven Framework for Dynamic Trust Management

Funmi Onolaja
Rami Bahsoon
Georgios Theodoropoulos

School of Computer Science
The University of Birmingham, UK

International Conference on Computational Science ICCS2011

UNIVERSITY OF BIRMINGHAM

Outline

- ✓ Trust and Reputation
- ✓ Reputation and trust-based models
- ✓ DDDAS inspired framework
- ✓ Case study/results
- ✓ Summary

Trust and Reputation

- ✓ **Trust**
- ✓ **Reputation**

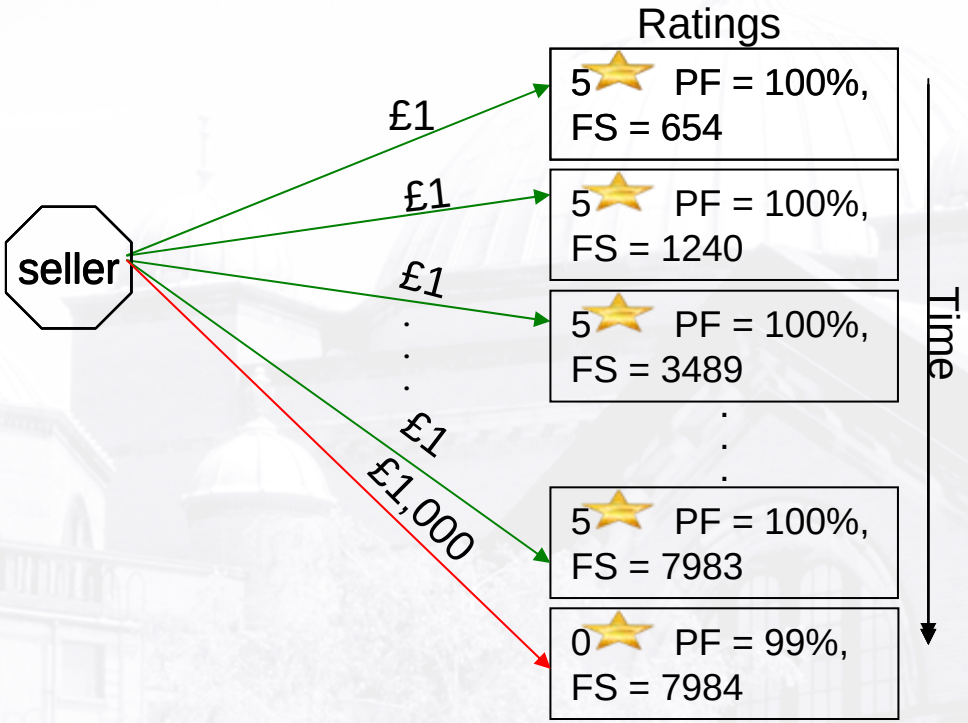
- ✓ **Trust management**

Reputation and trust-based models e.g
CORE, CONFIDANT, TrustGuard etc

- Domains
- Distinguish members
- Incentives / punishment
- Trust Values (TV)
- Watchdog (Collusion – trust decisions corrupted)
- Past histories (Intoxication)

Trust management: intoxication

- ✓ Assumption: predictive power depends on the supposition that past behaviour is an indication of future behaviour.
- ✓ Not true with *intoxication attacks.* Simple example, eBay.
- ✓ Difficult to identify - sudden misbehaviour.
- ✓ Effect of past good behaviour outweighs the effect of current actions on reputation.



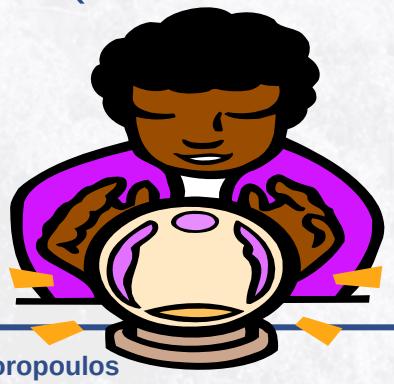
PF = Positive feedback ratings
FS = Feedback scores

Trust management: dynamic nature

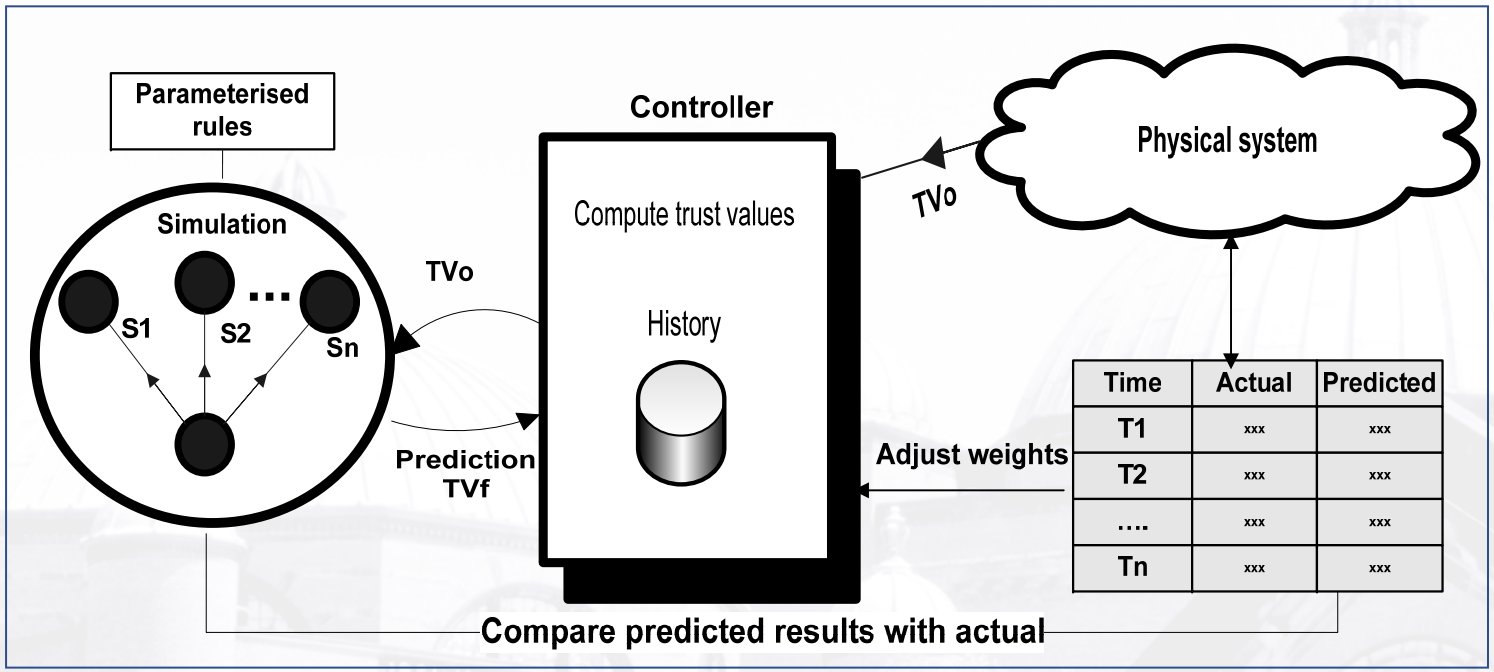
- ✓ Trust and reputation are not static but dynamic, computation of trust should be equally dynamic.
- ✓ Dynamic approach to identifying and isolating misbehaving (group of) members.

Requirements

- ✓ Dynamic online rating of members (data),
- ✓ Members' bias influencing trust decisions (as in the case watchdog) and
- ✓ Anticipate events and predict TVs.



Framework: components



Simulation

- ✓ Parameterised / behavioural rules
- ✓ Probabilities of collaboration / misbehaviour
- ✓ Scenario-based prediction of future ratings
- ✓ Focus of high risk members
- ✓ Compare with the real system and adjust weights (Feedback)

Real system

- ✓ Historical and recent online rating with weightings
- ✓ Qualitative data to quantitative value (Controller)
- ✓ Risk regions

Framework: trust values

$$tv^R = \mu_h tv_h^R + \mu_o tv_o^R$$

- ✓ Weights μ_h and μ_o - factors for the online and historical TVs.
- ✓ $[\mu_h, \mu_o] > 0$ and $\mu_o > \mu_h$, more emphasis on recent behaviour.

$$tv_f^S = \frac{(tv_o^S)\,S_1 + (tv_o^S)\,S_2 + (tv_o^S)\,S_3 + \cdots + (tv_o^S)\,S_n}{N}$$

$$TV = \mu_h tv_h^R + \mu_o tv_o^R + \mu_f tv_f^S$$

- ✓ tv_h^R, $tv^R{}_o$, $tv^S{}_o$ and $tv^S{}_f$ represent the historical, online TVs in the physical system, online TV in simulation and the predicted TV in simulation respectively.
- ✓ N is number of scenarios and $(S_1, S_2, \ldots Sn)$ are the scenarios.

Framework: trust table with level of risk

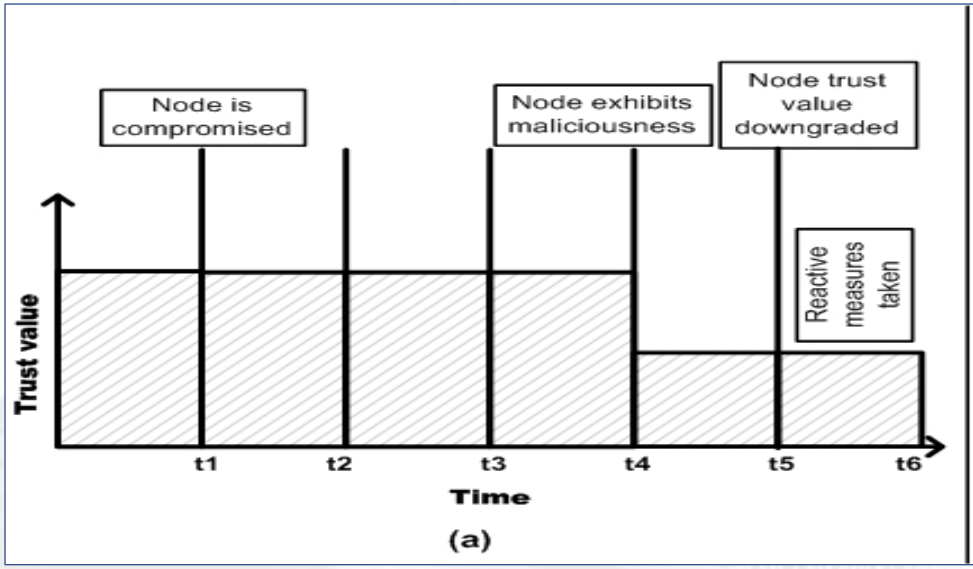
Trust table showing the degrees of trust and regions of risk

TV	Meaning	Description	Region
5	Complete trust	Trusted node with an excellent reputation	Low risk
4	Good trust level	Very reliable node	Low risk
3	Average trust level	Average value and somewhat reliable node	Medium risk
2	Average trust level	Average value but questionable node	Medium risk
1	Poor trust level	A questionable node	High risk
0	Complete distrust	Malicious node with a bad reputation	High risk

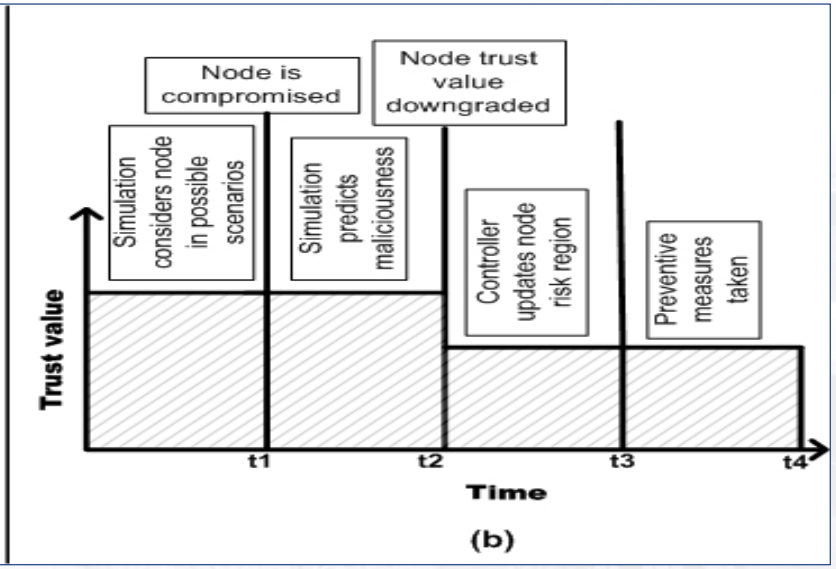
- ✓ Each value represents a degree of trust.
- ✓ Degrees of trust introduce flexibility into applications of our framework, as different behaviours correspond to different levels of trust.
- ✓ Region migration and reputation redemption takes longer.

Case study

Reactive



Proactive

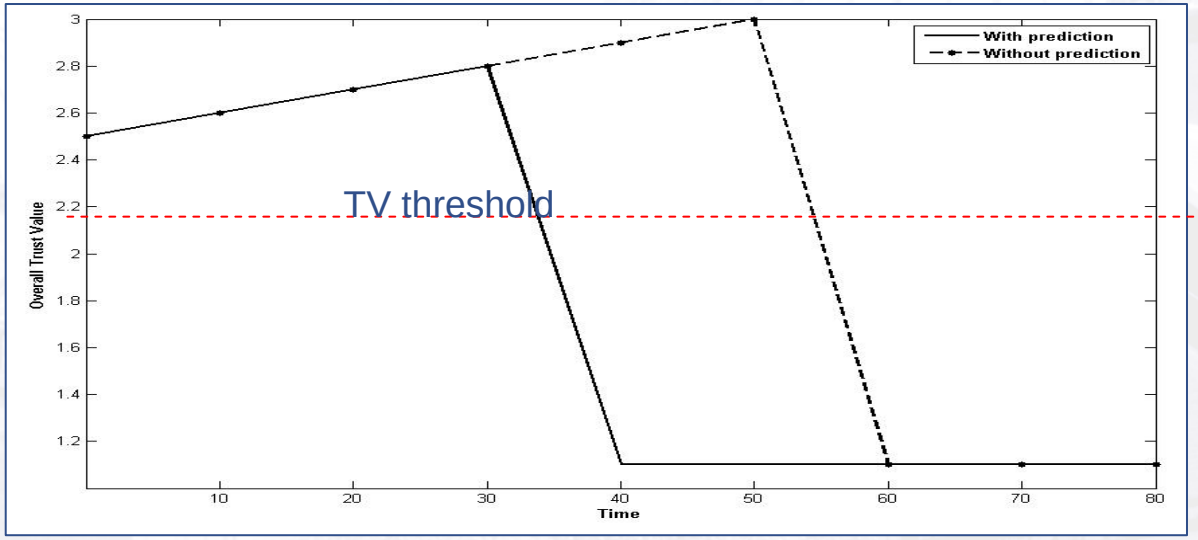


- ✓ Critical domains (P2P case study),
- ✓ The prediction gives the system enough time for preventive measures,
- ✓ Framework proactive compared to other models that are reactive in nature.

Case study

- ✓ Purpose: Test the performance the framework with and without prediction.
- ✓ Parameters: Maze p2p, 100 peers, 4% misbehave, 27 files transferred, μ_o = 0.5, μ_h = 0.3, μ_f = 0.2.
- ✓ Observation: Time difference of 20 ticks in identifying an intoxicating node.
- ✓ Lesson learnt: Framework has potential of better performance with prediction.

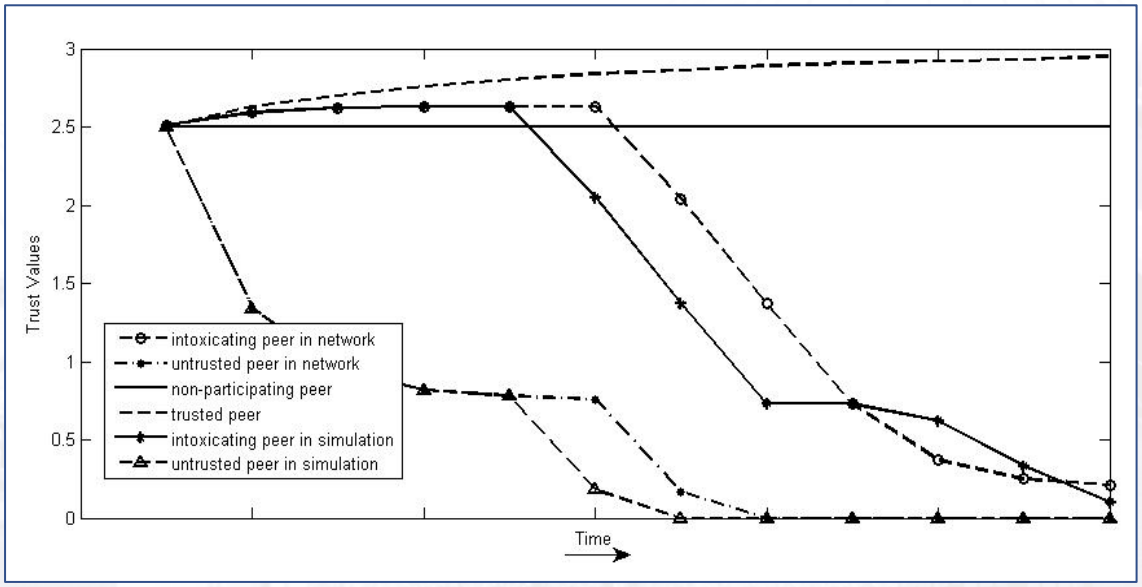
With prediction vs. without prediction



Case study

- ✓ Purpose: Compare real values with predicted values.
- ✓ Parameters: Maze p2p, 100 peers, 4% misbehave, 27 files transferred, μ_o = 0.5, μ_h = 0.3, μ_f = 0.2.
- ✓ Observation: Prediction not accurate but reflects reality.
- ✓ Lesson learnt: False positives and negatives.

Trust values of peers in the P2P network and simulation



Summary

- ✓ Framework has the potential of providing a high level of dynamism to trust and reputation systems allowing for a more realistic analysis of the system and enabling predictions.
- ✓ Results suggest that hypothesis is most likely correct based on the scenarios considered.
- ✓ Preventive mechanisms for avoiding collusion and intoxication attacks.
- ✓ Future challenges
  - Validation – accuracy of predictions, rate of false positives and negatives.
  - Evaluation of performance.
  - Emerging attacks.

Funmi Onolaja
o.o.onolaja@cs.bham.ac.uk