An Investigation into Trust and Reputation Frameworks for Collaborative Teams of Autonomous Underwater Vehicles

Andrew Bolster

University of Liverpool

andrew.bolster@liv.ac.uk

July 3, 2014

Research Context

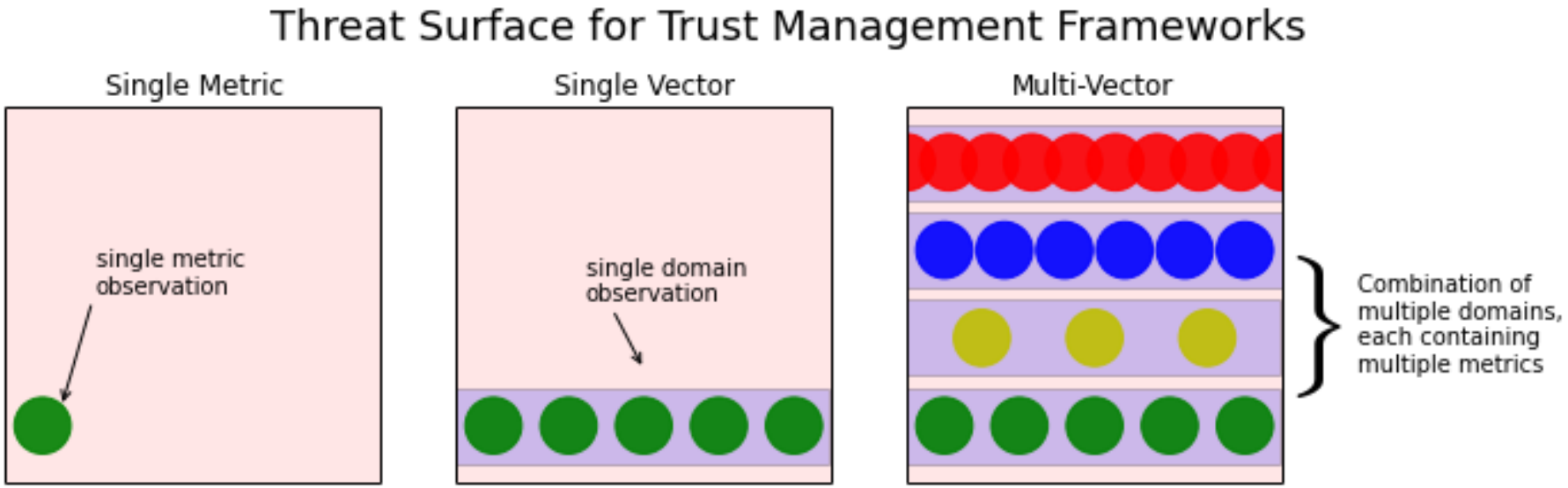
- Project launched at QUB ECIT in 2011 under the DSTL/DGA Anglo French Defence Research Group PhD Programme
- What lessons from the Mobile Ad Hoc Network (MANET) space can be transferred to the marine environment?
- Teams of 3 - 16 Autonomous Underwater Vehicles (AUVs) Mine countermeasures, Hydrography, and Patrol Capabilities (MHPC)
- Defence focus, assumption of highly capable enemy attempting to compromise communications / operations
- Primary Simulation/Analysis work done in 12/13
- Moved to UoL Oct 13 after 2 mth placement @ DSTL PDW Naval Systems / Information Systems departments.

Trust in Ad-Hoc Systems and the context of this document

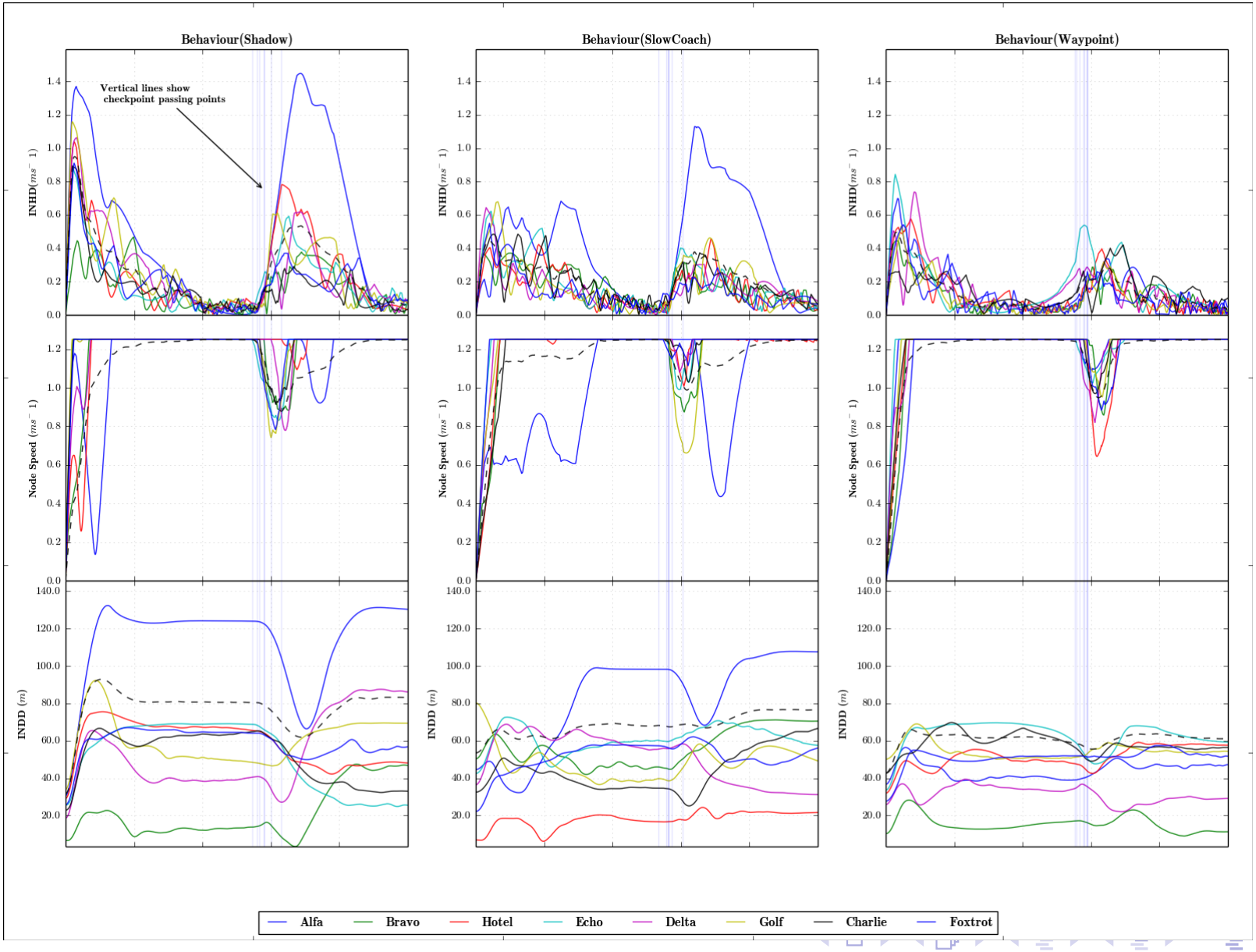
- Particularly interested in the application of Trust in Decentralised (P2P) Autonomous Systems of Systems, AUVs for example
- Trust: *The expectation of an actor performing a certain task or range of tasks within a certain confidence or probability*
- Full System Views of Trust
  - Design Trust - a system of systems will perform as designed
  - *Operational Trust - an individual system will perform as designed in field*
- Communications not the only target for an attacker (or failure);
  - Following to restricted area
  - Masquerading
  - Hardware Degradation
  - Resource attack via propulsive power
- Physical observation as opportunity to reduce the threat surface while discriminating between 'True' attacks and mechanical failure.
- Also could provide additional 'handshake' protocols for 'friendly' fleets/teams through reactionary behaviours

Multi-Vector Trust and the Threat Surface

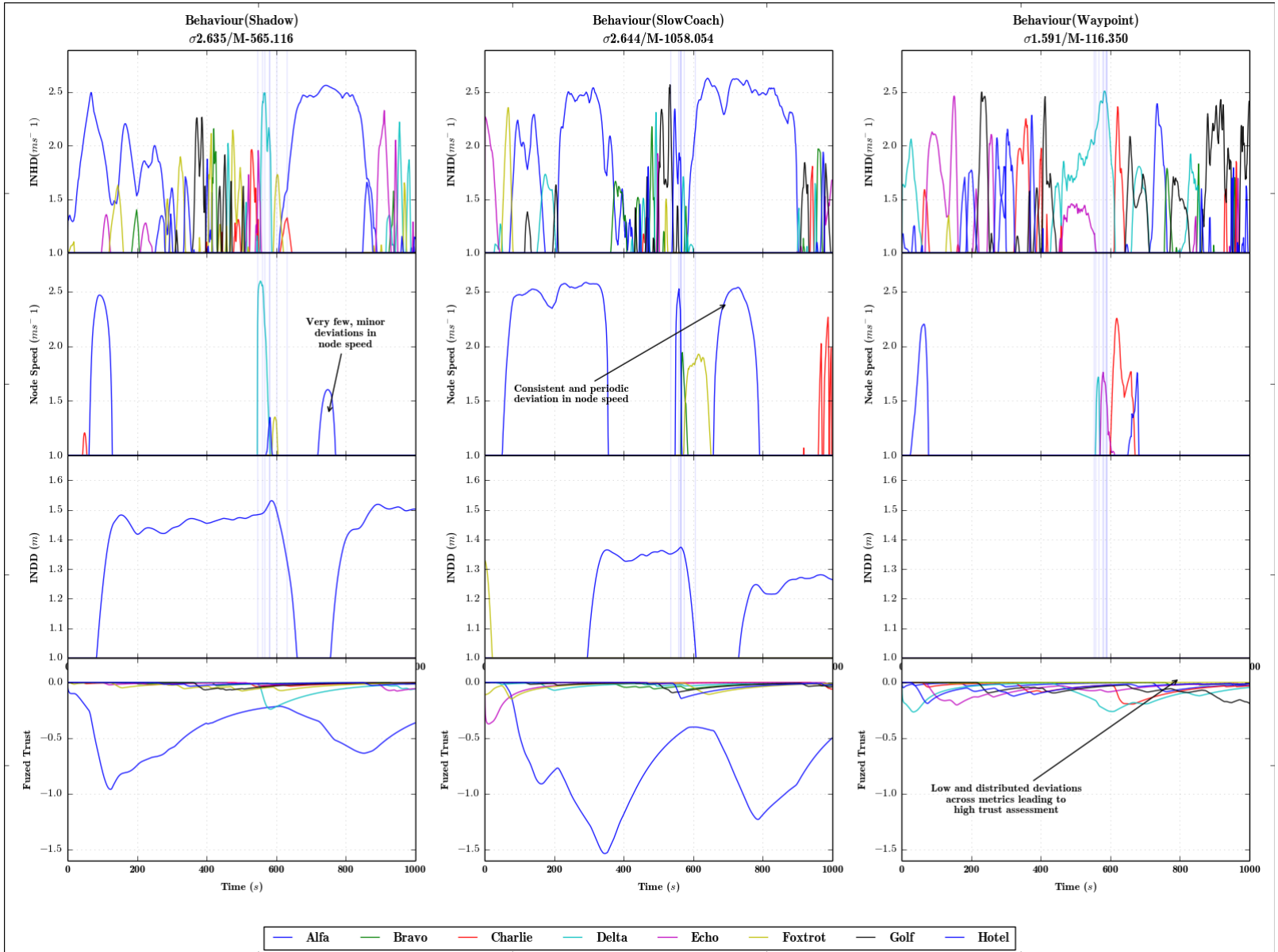
Potential attacks exist across a multi-domain threat surface



Raw Behavioural Metric Assessment in AUVs



Behavioural Trust Assessment in AUVs



Behavioural Trust Assessment in AUVs

- Detection and identification based on basic weight-assessment classifier against windowed history of observations, with confidence based on a Grey Theoretic weight
- Currently >96% statistical accuracy of detection and confidence, but this needs much more rigorous analysis
- Challenges to Trust assessment
  - How to define optimality in trust assessment when dealing with multiple vectors and transitive trust?
  - Is there a quantifiable benefit to cross-domain comparison beyond single vector Trust?
  - Is there an optimal generic cross-domain comparator?

Current Publications

- A Multi-Vector Trust Framework for Autonomous Systems [2]
  - Symposium paper to the Association for the Advancement of Artificial Intelligence on the current state of work, presenting our progress towards multi-vector trust
- Analysis of Trust Interfaces in Autonomous and Semi-Autonomous Collaborative MHPC Operations [1]
  - Part of a Five-Eyes defence strategy programme (TTCP) for assuring C3I capabilities as part of FF2020

Development Plan

1. Behaviour Detection (Q3 14) - Formal Analysis of Behavioural Trust Systems
   - INFOCOM 2015 (Aug 14)
   - ASON 2014 : Seventh Int. WS on Autonomous Self-Organizing Networks (Aug 14)
   - AHUC 2014 : The Fourth Int. WS on Ad Hoc and Ubiquitous Computing (Aug 14)
   - ICCAR 2015 : WASET Int. Conf. on Control, Automation and Robotics (Dec 14)
2. MANET/Marine comparison (Q4 14) - Formal Comparison between Terrestrial MANET / Marine contexts
3. Multi-Domain Trust Assessment (Q4 14) - Combination of Communicative and Physical Behaviour Trusts
   - IEEE Trans. on Communications / Dependable and Secure Computing / Intelligent Systems
4. Reactionary/Perturbative Trust (Q1 15) - Exploration of reactionary behaviours for teams to 'shake down' suspects
   - SASO15:Self-Adaptive and Self-Organizing Systems,
   - SEAMS15: Software Engineering for Adaptive and Self-Managing Systems

Research Collaborations

- DSTL
  - Visits and Placements (Summer '13) at DSTL Porton Down and Portsdown West
  - CDE Exhibition, London, (Spring '12)
  - PhD National Conferences, Oxford and London (12/13)
  - Direct Contribution to 5-Eyes programme on Autonomous Systems (13/14)
- DGA/UPMC
  - DGA Conference (Autumn, '12)
  - Visits fo CRIIF (Autumn, '12)
- NATO/CMRE
  - UComms'12
  - Visits & Ongoing data sharing with CMRE(NURC) in La Spezzia
- NPL/Plextek
  - CDE Project on Precision Timing for Positioning with NPL/Plextek
  - Simulation and Analysis of relevant drift characteristics; increasing positional accuracy by 40%

Research Experience

- Project launched at QUB ECIT in 2011 under the DSTL/DGA Anglo French Defence Research Group PhD Programme
- Primary Simulation/Analysis work done in 12/13
- Moved to UoL Oct 13 after 2 mth placement @ DSTL PDW Naval Systems / Information Systems departments.

Difficulties

- Move to UoL was challenging mid programme: new structures, requirements, etc. Incurred Delays
- Access to secure materials difficult (although placement helped a lot).
- Multiplicity of reporting (UoL, DSTL, Joint Programme, etc)

Benefits

- Flexibility in travel enabled international collaboration within and outside partners
- DSTL Placement extremely useful for context and background verification

References I

Andrew Bolster. *Analysis of Trust Interfaces in Autonomous and Semi-Autonomous Collaborative MHPC Operations*. Tech. rep. The Technical Cooperation Program, 2014.

Andrew Bolster and Alan Marshall. "A Multi-Vector Trust Framework for Autonomous Systems". In: *2014 AAAI Spring Symposium Series*. Stanford, CA, 2014, pp. 17–19. URL: http://www.aaai.org/ocs/index.php/SSS/SSS14/paper/viewFile/7697/7724.

The End