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

Andrew Bolster

University of Liverpool

andrew.bolster@liv.ac.uk

UNIVERSITY OF LIVERPOOL

June 17, 2015

1. Issues
2. Aims
3. Approach
4. Impact

Context

- Increasing use of Autonomy in Underwater Acoustic Networks
- Extremely constrained communications/processing/power
- Drive towards smaller, disposable, decentralised systems of systems for applications in MHPC in defence, petrochemical, and environmental applications

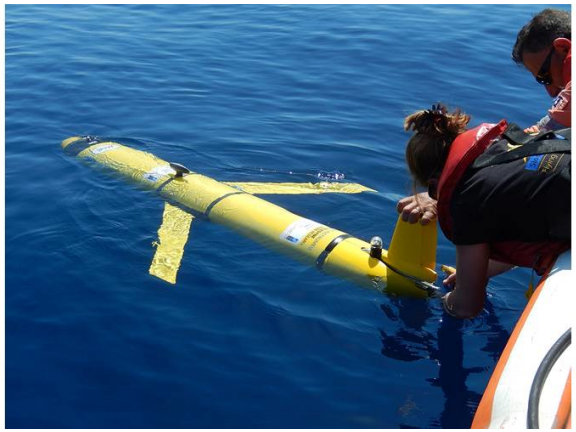

Fig. 1: REMUS 100 AUV at CMRE: Potential target application

Adoption of open interoperability stds. and "CoTS" procurement pipelines

Novel and unique threats to trust and security

Open Questions

- **Centralised** security difficult/expensive to maintain
- Presents **single-point-of-failure** for operational support
- Move from Centralised to Distributed trust management already demonstrated in Terrestrial **MANETs**
- Constrained comms. make comms. only monitoring non-optimal

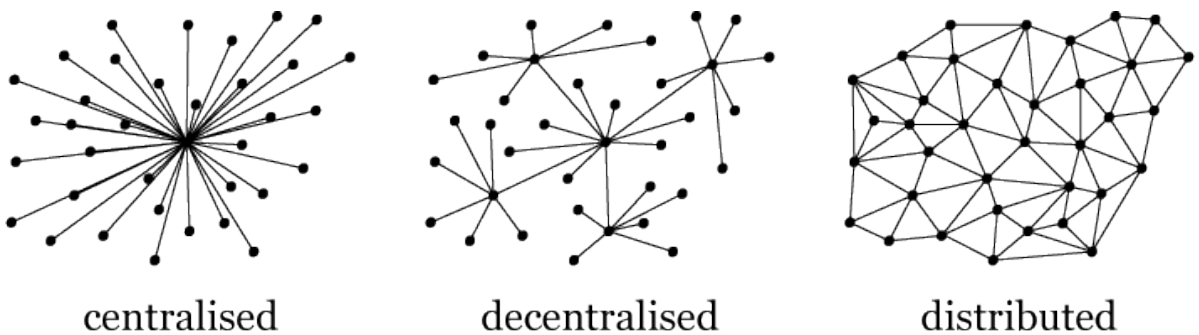

Fig. 2: Autonomy is driving increasingly towards distributed applications

Can these MANET techniques be applied to the **marine context**?
What metrics can be used to establish and maintain distributed trust?

Trust Management in Marine Networks

- Comms. only Trust Management Frameworks (TMFs) in MANETs
- Generally **Bayesian Estimation** of binary success/fail observation
- Not stable in **sparse, variable, & noisy** environments
- Can (generally) only detect misbehaviour, not classify
- Only detects packet-dropping misbehaviours
- Recent work uses multiple, continuous, measurements (e.g. *SNR, Delay, Throughput, PLR*) utilising Grey Theory[1] to form a trust "**vector**"
- Provides **multi-dimensional classification** of misbehaviour

Novelty

- **Assess** existing approaches in simulated UAN, characterising their bounds of suitability/performance
- **Extend** multi-metric approach to encompass **physical behaviours** as well as comms.
- Treat threat surface as a multi-dimensional constraint space, aiming to restrict and protect operations

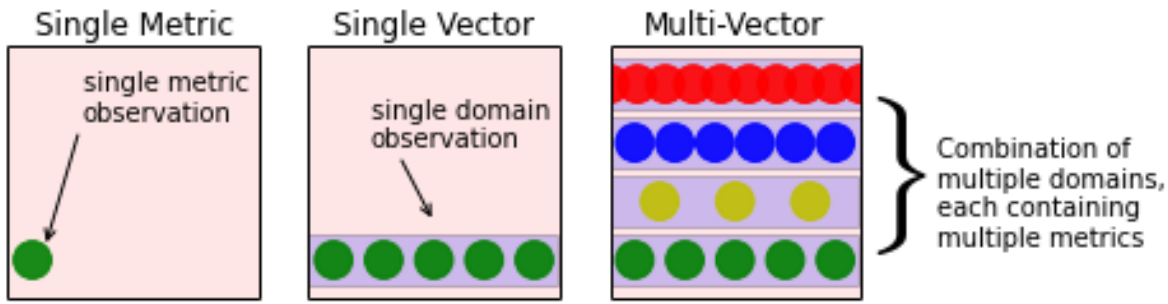

Fig. 3: The available threat surface can be protected through extending trust observations across multiple types of observation

Current Results

- Demonstration of PoC TMF utilising Behavioural Metrics
- Protocol for identification/assessment of metric suitability across several misbehaviour types
- Performance assessment of Hermes, OTMF, and MTFM in simulated marine environment
- Information theoretic assessment of multi-domain combination strategies

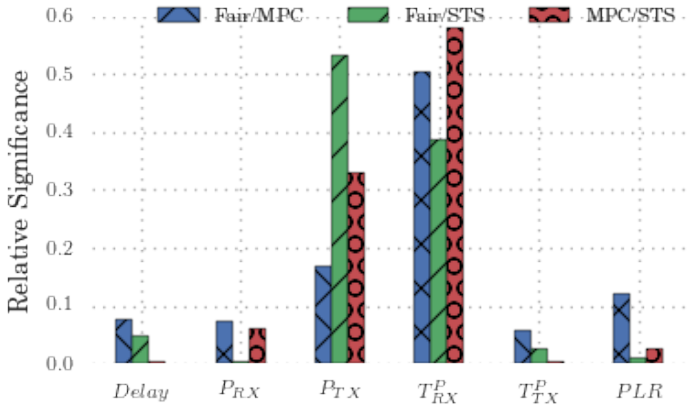

Fig. 4: Factor Analysis of Malicious, Selfish and Fair behaviours

Current Outputs

- Summer Research **Placement with DSTL** (Software Systems and Dependability for Autonomous Teams/Naval Systems Group)(2013, PDW)
- **Paper** Presentation to the Association for the Advancement of Artificial Intelligence (AAAI) (Stanford, USA) [2]
- **Technical Report** for the UK/US/CAN/AUS/NZ Technical Cooperation Programme [3]
- DSTL **CDE Collaboration** with NPL and Plextek Ltd. on "Precision Timing and Navigation, Resilient Time and Location Estimation for Networked Assets" (CDE 33135)
- **Paper** Presentation to the IEEE International Symposium on Recent Advances of Trust, Security and Privacy in Computing and Communications (TrustComm, Helsinki, FI) [4]

Future Impacts

- Advisory factor to FF2020 on application & verifiability of **in-field autonomy**
- Deployment of smaller/cheaper collective assets, through **lowering comms overheads**
- Increase viability / **confidence** for "stand-off" MCM
- Increased **reliability** of autonomous/mixed SoS through continual self-policing
- Applications beyond marine; applicable to any constrained / DTN as well as to virtual/**cyber-physical systems** (i.e. the application of these methods to abstract metric domains)

References I

Ji Guo, Alan Marshall, and Bosheng Zhou. "A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks". In: *Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011* (2011), pp. 142–149. DOI: 10.1109/TrustCom.2011.21. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120813.

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

References II


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. "Single and Multi-Metric Trust Management Frameworks for use in Underwater Autonomous Networks". In: *TrustCom2015*.

The End