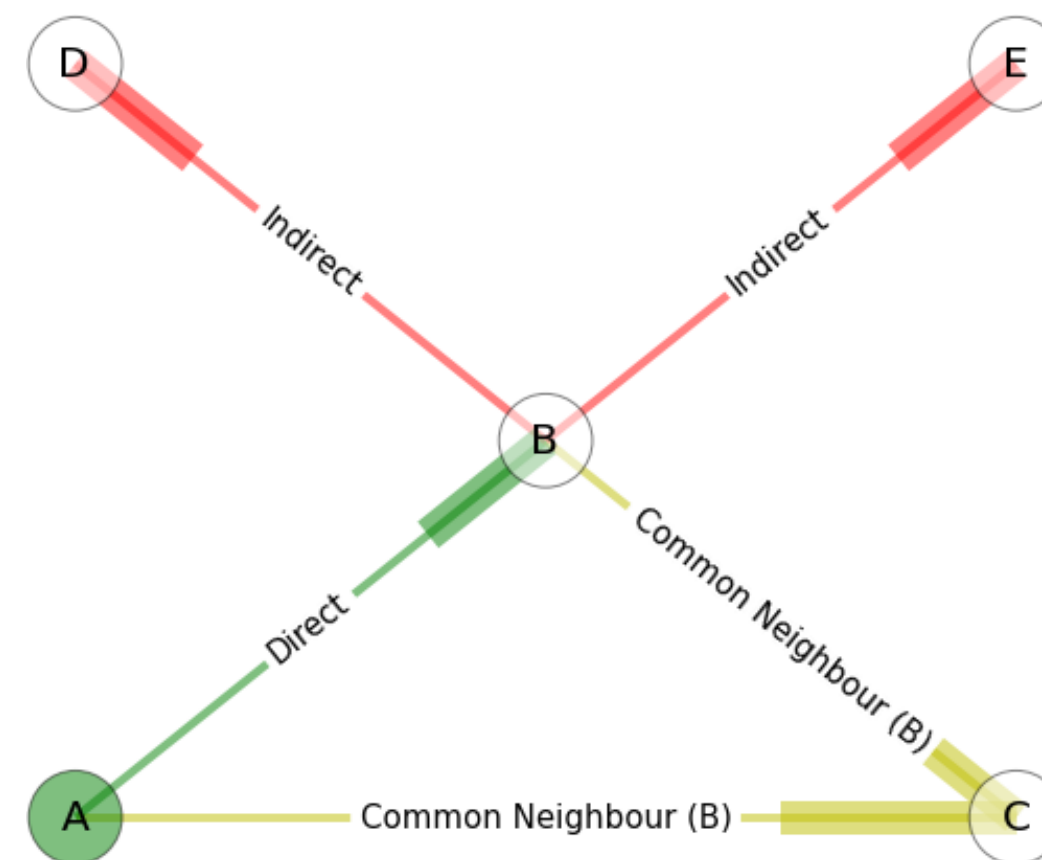
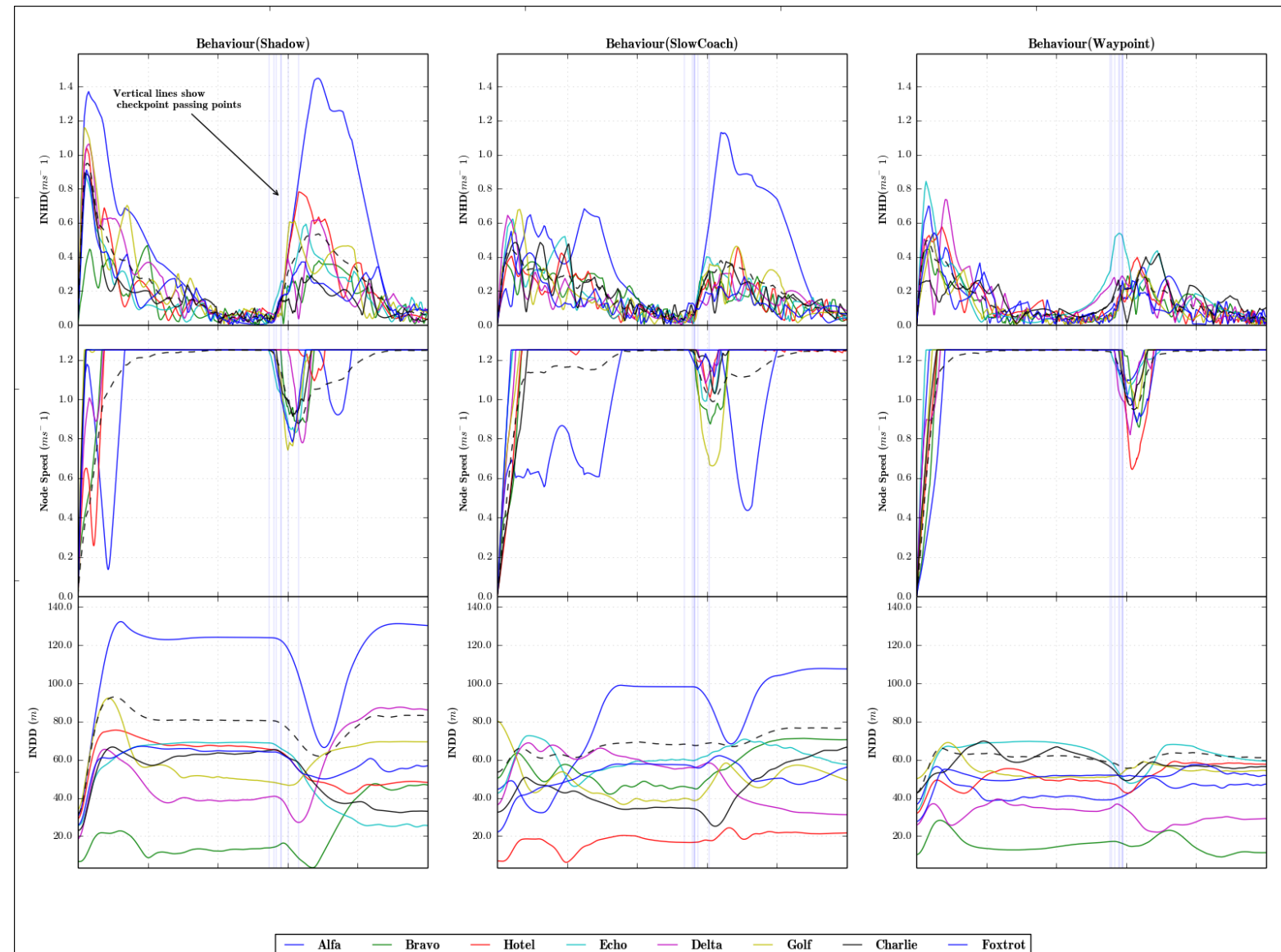
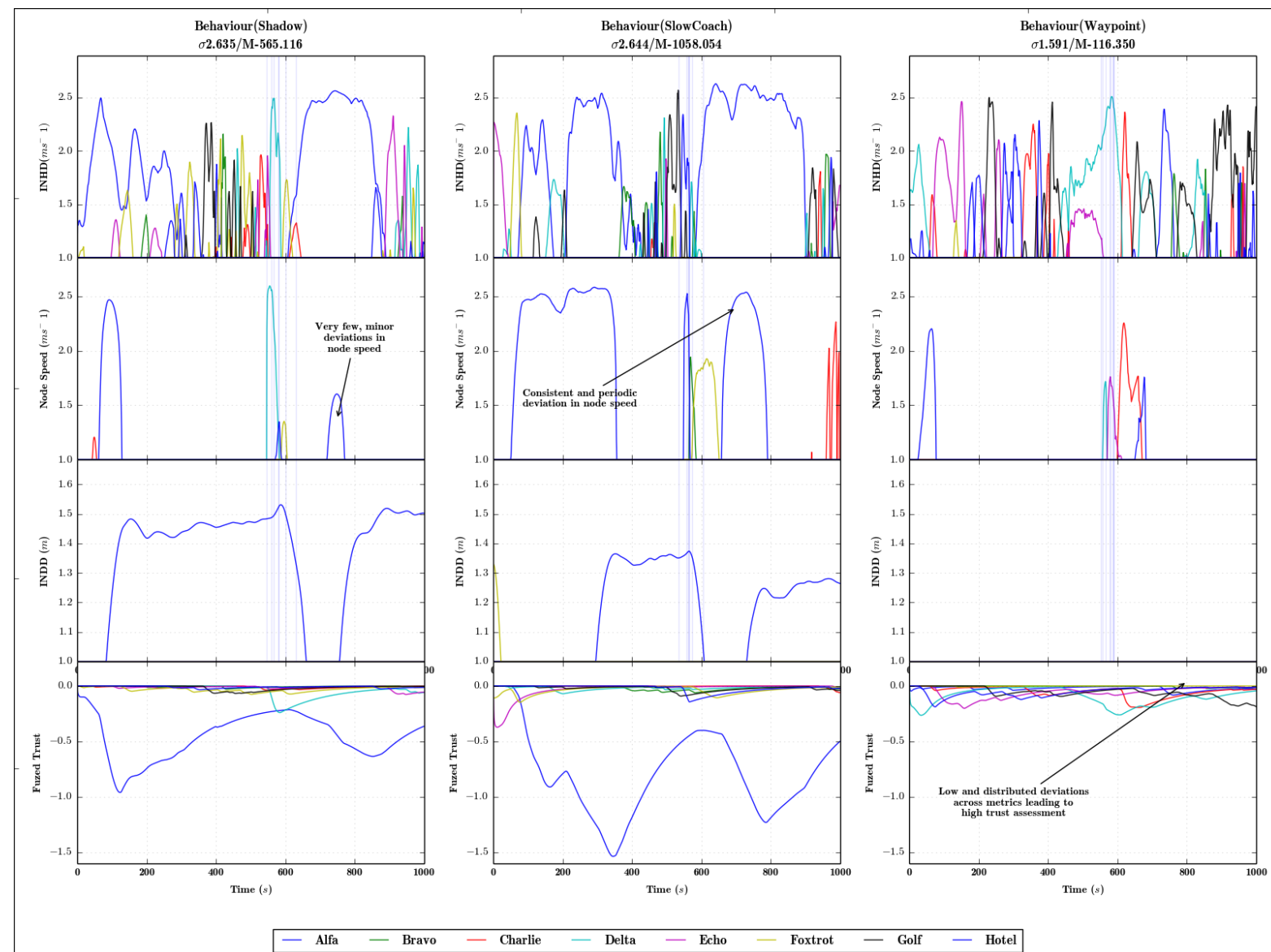

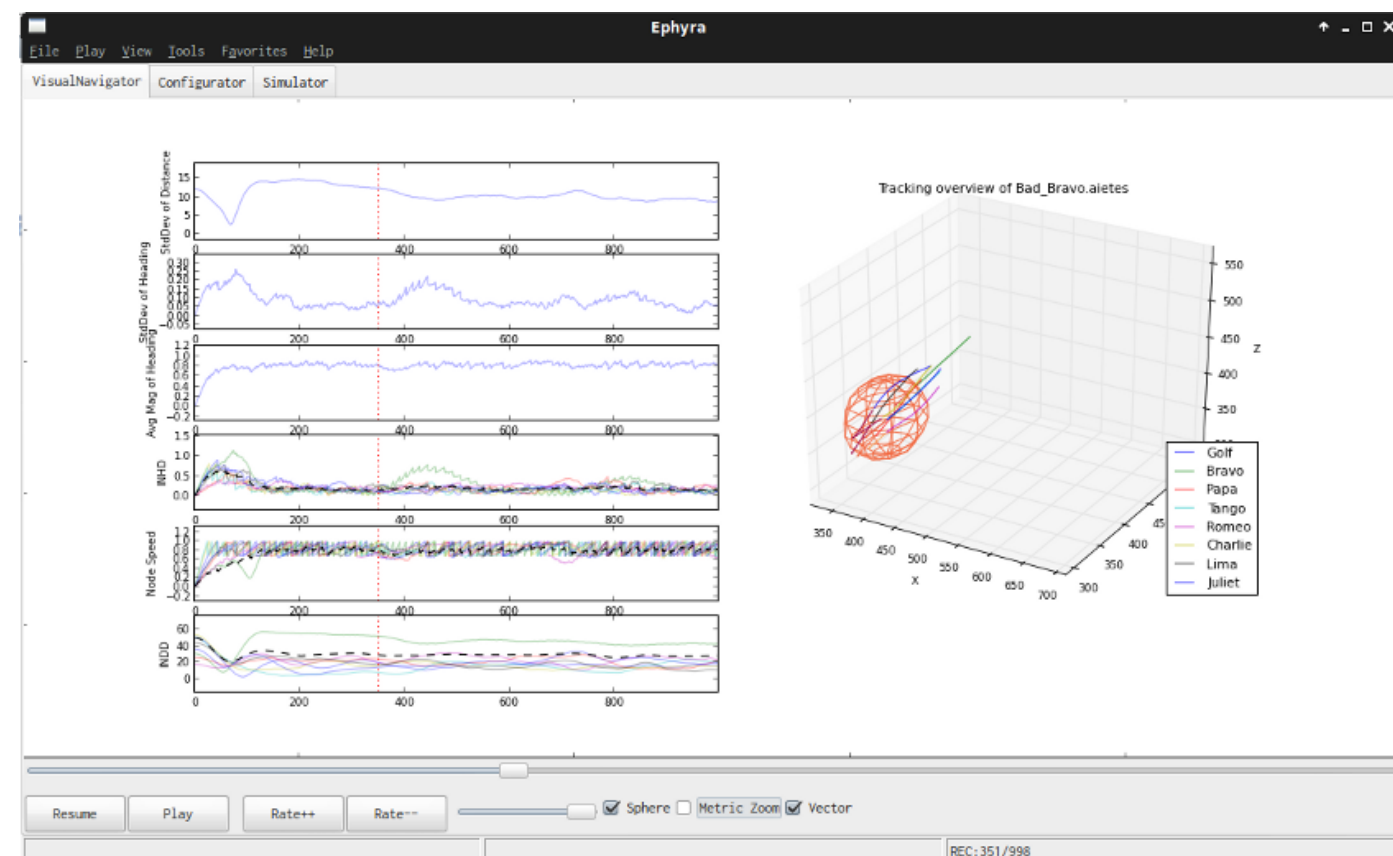


| | | | | |
|--|---|--|---|--|
| <div>Project Background</div> <div><ul style="list-style-type: none">► Project launched at QUB ECIT in 2011 under the DSTL/DGA Anglo French Defence Research Group PhD Programme► What lessons from the Mobile Ad Hoc Network (MANET) space can be transferred to the marine environment?► Teams of 3 - 16 Autonomous Underwater Vehicles (AUVs) with 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.► CDE Project on Precision Timing for Collaborative Acoustic Positioning with NPL/Plextek</div> | <div>Trust Management Frameworks (TMFs)</div> <div><p>TMFs are protocols designed to provide information regarding the estimated future states and operations of nodes within networks</p><p>“[...]collecting the information necessary to establish a trust relationship and dynamically monitoring and adjusting the existing trust relationship” - [1]</p><p>Enables nodes to form collaborative <i>opinions</i> on their cohort nodes based on</p><ul style="list-style-type: none">► Direct Observation of Communications Behaviour (eg Successfully Forwarded Packets)► Common-Neighbour Recommendation► Indirect Reputation<p>Multiple transitive relationships can be maintained over time, providing trust resilience with dynamic network topologies</p></div> <div>Figure 2: Direct, Recommendation, and Indirect trust relationships</div> | <div>Malicious Behaviours</div> <div><p>A series of 'Malicious' behaviours have been designed, where one or more nodes were actively attempting to compromise the fleet in some way.</p><ul style="list-style-type: none">► <i>Shadow</i> - Following the fleet without restricted mission data► <i>Spy</i> - A node that intermittently rises in the fleet, potentially surfacing to relay mission information to a third party► <i>Sloth</i> - Selfish conservation of energy by taking minimal paths► <i>Stalker</i> - Tailing a specific node, attempting to use this consistent history to poison the trust network► <i>Scountrel</i> - Falsely reporting its estimated position with the intention to corrupt a collaborative positioning system or induce a collision<p>Additionally, there are non-malicious behaviours, the classification of which is equally important in separating friend from foe.</p><ul style="list-style-type: none">► <i>Slow Coach</i> - Where a node's power train is damaged, causing reduced maneuverability and performance► <i>Spin Doctor</i> - Damage to control surfaces or to Inertial Navigation System</div> | <div>Analysis Cont.</div> <div></div> <div>Figure 5: Per-Simulation metric measurements for Malicious, Impaired, and Control behaviours (Shadow, SlowCoach and Waypoint)</div> <div><p><i>INDD</i> is an obvious candidate for a suspicion 'trigger', but looking at <i>INHD</i> values after a few hundred seconds of simulation time; an anomaly is clearly being detected.</p><p>In addition, <i>Alfa</i> node (the Blue Line) is clearly an outlier in terms of <i>INHD</i> and <i>Node Speed</i> in the earliest sections of the graph, at which point nothing appears to be out of the ordinary in <i>INDD</i>. This implies that a fusion of metrics would be more effective than a simple detection envelope on a single metric.</p></div> <div>Figure 6: Per-Node deviations for each metric, with an additional row showing an EWMA based cross-metric trust assessment. Note the different in 'Node Speed' triggers between the malicious and impaired behaviours</div> <div><p>Considering the Baseline data (Right side of Figure 5), it's clear that these metrics are not infallible, as is demonstrated by the number of relatively short-lived false positives, demonstrating the need to use multiple metrics for reliable trust assessment.</p><p>Figure 6 demonstrates a windowed, weighted trust fusion, where deviations in individual metrics are combined to generate a Trust Value.</p></div> | <div>Conclusions</div> <div><p>This research area presents a range of challenges and opportunities within both civil and defence operations; an auditable trust framework for automated marine craft would be a significant enabling factor to the roll-out of more low-maintenance or even “Fire and Forget” deployments for persistent patrol/monitoring tasks.</p><p>Open Hypotheses in this field that this project intends to answer are:</p><ul style="list-style-type: none">► How can optimality in trust assessment based on behaviour be defined win a distributed, dynamic network topology?► Is there a quantifiable benefit to cross-domain comparison beyond single-vector trust? (i.e. 1-D vector vs cross domain comparison)► Is there an optimal <i>generic</i> cross domain fusion methodology?</div> <div>Current Publications</div> <div><ul style="list-style-type: none">► A Multi-Vector Trust Framework for Autonomous Systems [2]<ul style="list-style-type: none">▷ 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 [3]<ul style="list-style-type: none">▷ Part of a Five-Eyes defence strategy programme (TTCP) for assuring C3I capabilities as part of FF2020</div> <div>Development Plan</div> <div><ul style="list-style-type: none">► Behaviour Detection (Q3 14) - Formal Analysis of Behavioural Trust Systems<ul style="list-style-type: none">▷ 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)► MANET/Marine comparison (Q4 14) - Formal Comparison between Terrestrial MANET / Marine contexts► Multi-Domain Trust Assessment (Q4 14) - Combination of Communicative and Physical Behaviour Trusts<ul style="list-style-type: none">▷ IEEE Trans. on Communications / Dependable and Secure Computing / Intelligent Systems► Reactionary/Perturbative Trust (Q1 15) - Exploration of reactionary behaviours for teams to 'shake down' suspects<ul style="list-style-type: none">▷ SASO15:Self-Adaptive and Self-Organizing Systems,▷ SEAMS15: Software Engineering for Adaptive and Self-Managing Systems</div> <div>Bibliography</div> <div><ul style="list-style-type: none">► Huaizhi Li and Mukesh Singhal. “Trust Management in Distributed Systems”. In: <i>Computer</i> 40.2 (2007), pp. 45–53. ISSN: 00189162. DOI: 10.1109/MC.2007.76. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622.► Andrew Bolster and Alan Marshall. “A Multi-Vector Trust Framework for Autonomous Systems”. In: <i>2014 AAAI Spring Symposium Series</i>. Stanford, CA, 2014, pp. 17–19. URL: http://www.aaai.org/ocs/index.php/SSS/SSS14/paper/viewFile/7697/7724.► Andrew Bolster. <i>Analysis of Trust Interfaces in Autonomous and Semi-Autonomous Collaborative MHPC Operations</i>. Tech. rep. The Technical Cooperation Program, 2014.</div> |
| <div>Introduction</div> <div><p><i>Aim of project:</i> To use physical behaviours and observations to assess and maintain trust within mobile, marine, ad-hoc networks</p><p>Small fleets of AUVs (<i>Autonomous Underwater Vehicles</i>) will be expected to operate in isolated environments.</p><p>This requires an auditable sense of trust within the remote intra-fleet communications networks, incorporating</p><ul style="list-style-type: none">► Communications Activity► Mission Suitability/Capability► Behavioural Monitoring<p>The use of centrally coordinated trust models presents a single point of failure.</p><p>Secure communication in marine environments is expensive and time consuming; adopting a decentralised form of trust assurance will reduce these costs by localising the per-node security environment.</p></div> <div>Figure 1: REMUS 100 AUV, as deployed at CMRE, a potential target platform for this work</div> | <div>The Need for Multi-Domain Trust in Autonomous Systems</div> <div><p>Communications not the only target for an attacker (or failure);</p><ul style="list-style-type: none">► Following to restricted area► Masquerading► Hardware Degradation► Resource attack via propulsive power<p>Physical observation presents opportunity to further reduce the available threat surface while also discriminating between 'True' attacks and mechanical failure.</p><p>Also could provide additional 'handshake' protocols for 'friendly' fleets/teams through reactionary behaviours</p><p>Potential attacks exist within a multi-domain threat surface, and as further metrics and domains of trust are included in a TMF, attackers are increasingly restricted in their behaviour until the only way to avoid detection is to behave correctly.</p></div> <div>Figure 3: Threat Surface for Trust Management Frameworks</div> | <div>Proof of Concept Analysis</div> <div><p>The aim of the Proof of Concept is to demonstrate not only the detection capability of using behavioural metrics to access trust but to differentiate between malicious and impaired behaviours.</p><p>Three fleets are simulated performing a simple patrol mission, each with a particular behaviour set. The first has a malicious node performing a 'Shadow' behaviour, representing a malicious outside actor attempting to infiltrate the fleet. The second has an impaired node exhibiting 'SlowCoach' behaviour, representing a damaged or faulty but otherwise good node.</p><p>The simulations were run to for a standard eight hour mission time, with three primary metrics being assessed at run time by each node:</p><ul style="list-style-type: none">► <i>INHD</i>: Inter Node Heading Deviation, or the per-node deviation from the fleet-average velocity vector► <i>Node Speed</i>: The Magnitude of Velocity of each node► <i>INDD</i>: Inter Node Distance Deviation, or the normalised deviation between the inter-node distance matrices from the perspective of each node</div> <div>Figure 4: The Ephyra visualiser allows for rapid modelling and analysis of node data, as well as overlay information on individual and fleet behaviours and metrics.</div> | <div>Future Applications</div> <div><ul style="list-style-type: none">► Due to the high communications, motion, and computation costs, and lack of external location reporting (e.g. <i>GPS</i>), behavioural analysis in the marine environment is particularly difficult, but if successful, can be reliably applied in a wide variety of fields including but not limited to<ul style="list-style-type: none">▷ Self-Driving Cars▷ Environmental Survey drones (terrestrial, marine, and aerial)▷ Satellite Communications Arrays▷ Internet Certificate Authority verification▷ Verifiable Distributed Computing</div> | |