An Investigation into Trust and Reputation Frameworks for Autonomous Underwater Vehicles

Andrew Bolster
Institute of Electronics, Communications and Information Technology (ECIT)
Queen's University Belfast (QUB)

A documented submitted for
Initial Speech to DSTL on research progress
2011 November

0.1 Document Preamble

This document is intended to be verbally presented, as such its tone is informal. Subsection headings and **emboldened** are not intended to be spoken and indicate slide transitions.

0.2 Introduction

0.2.1 Title Slide

Good afternoon ladies and gentlemen, its an honour to be invited to present our project here, and I hope you find it both intriguing and enjoyable.

0.3 AUVs

0.3.1 AUV Definition

The general area of research selected is the commercial, defence, and environmental use of interdependent groups of Autonomous Underwater Vehicles, hereafter described as fleets.

0.3.2 Predators

After over 20 years of theoretical and exploratory research into Unmanned Vehicles on, above, and below sea level, the recent in-theatre use of UAVs such as the USAF's Predator range, has proven the effectiveness of autonomous or semi-autonomous ordnance delivery and reconnaissance platforms, and this success has opened the field of research to a much wider range of applications and platforms.

0.3.3 Predators + AUV

One area of particular interest to the research community has been the movement of ideas and technologies proven in the skies to the marine environment.

0.3.4 UAV Examples

Of particular interest to the research community is research into swarming behaviours of small reconnaissance drones, analogous to flocks of birds; human-guided operation, where by a remotely operated drone is flanked by a team of automated drones; and the use of task 'checkpointing' where by automated drones perform a particular task or series of tasks, and then notify a remote operator to take over manual control for specific roles.

0.3.5 AUV Examples

Bringing these type of technologies into the Naval space has led to applications such minefield detection and monitoring, submarine tracking, long range reconnaissance, deep-sea surveying, and much more. Earlier this year, successful trials were performed by NURC at La Spezia in Northern Italy investigating the collective performance of AUV's in port-protection in a counter-terrorism operational context.

The major foci of academic research into the use of autonomous robotics in a marine environment have been the development of individual and pre-defined group behaviour patterns within a fleet. However, the project introduced here addresses an important and emerging area; the incorporation of communications 'trust' to improve the operational effectiveness and reliability of such fleets.

0.4 Trust and Reputation Management

0.4.1 Trust

The question of trust is an important one; it is the quantitative assessment of the expected behaviour of a network node, in this case an individual AUV. This internal trust is generally robust and indeed secures the node network further where by each node is sharing trust information about its neighbouring nodes. This leads to the two basic trust mechanisms; direct and indirect recommendations. For instance, Nicola, you can communicate directly with Paul, and Paul can communicate directly with Alan, and as such, Nicola can speak from direct experience to the trustworthiness of Paul, and Paul of Alan. If Nicola wants to query Paul as to the trustworthiness of Alan, Paul can respond with his trustworthiness of Alan. Nicola; you then factor in your trust of Paul to find an indirect trust association of Alan, even if you've never interacted with him. Further, implied reputation can be garnered by association, so for instance I know Nicola you went to Strathclyde, and I have friends at Strathclyde who tell me its brilliant, I can therefore imply some reputation from that. In the reverse, you may have knowledge of Queen's, or of Professors Marshall or Fontaine, and by my association with them that may imply some qualatative reputation of me.

All of these different trust assessments, taken from multiple chains of trust can be used to generate trustworthiness values across many paths. This transfer of trust knowledge is usually described as multipath propagation.

This raises an important question; how does one assess the trust of a fleet-foreign entity of which no fleet-member has experience of?

0.4.2 Fleet Network

Taking the example of independent task-oriented operation, whereby fleets of AUVs operate autonomously over extended periods, independently from any persistent 'mother-

ship', this fleet may need to occasionally communicate with friendly ships or relay bouy's to return data for analysis or simply to notify task-commanders to their status. This raises the point just stated of how do we assess the trustworthiness of these extra-fleet entities such as the relay bouys or 'friendly' ships.

Additionally, the fleet will have significant internal communications between individual AUVs. In the case of above-sea-level UAV communication systems, this would simply be over free-space radio, but the marine environment creates significant challenges to even localised communications, due to factors such as low channel bandwidth, scattering, and long propagation delays.

As such, multiple technologies must be applied to enable underwater communications, including free-space optical and acoustic transmission systems, while radio is reserved for surface or very short range applications. These conditions make it very difficult to assess the real trustworthiness of an entity when it is unclear if its abnormal behaviour is due to these effects, or due to actual bad behaviour.

0.4.3 Loner

Further, due to the extended mission times of such fleets, and their planned isolation from classical command and control structures, they necessarily become vulnerable to attacks to subvert their objective; or to obtain or otherwise compromise the information they intend to report.

0.4.4 Healthy fleet

Additionally, the size of the fleet can be variable over time; with defective or otherwise incapacitated units 'dropping off' **(Dead Battery)-(fleet 4)** and fresh or specialised units being rolled out in-theatre **(fleet 6)** to join a particular fleet. This presents two major vulnerabilities; enemy emulation of a friendly mother-ship, or of a fleet individual.

0.4.5 Evil fleet

These factors taken together present two key challenges for a fleet; the ability to assess trust of a 'friendly' vessel, and to collectively detect potentially abnormal behaviour of a fleet-member.

It is these challenges that are the driving force of the proposed research. To date there has been little or no vulnerability analysis of fleets of AUVs. This project initially seeks to identify a range of threat models for fleets of autonomous AUVs; representative of real-mission events, for instance; passive eave's-dropping of communications; fleet infiltration using cloned AUVs or surface vessels; or partial fleet destruction to compromise mission capabilities.

0.4.6 MANETS

These threats have similarities to those experiences by wireless mobile ad-hoc and peer-to-peer networks, usually summarised as MANETs. Therefore a key initial area will be to investigate the applicability of existing research in those areas to the stated problem context. This would include research into existing modelling techniques as well as any protocols and behaviours used to counter these threats in the MANET space.

Any discussion of trust within this context leads to the need for a distributed trust and reputation management framework, using past experience to gauge the expected behaviour of a node in a distributed network. Most of these systems, such as Objective Trust Management Framework or OTMF, **OTMF Def** use only one physical or protocol measurement to make these trustworthiness decisions, but recent work has applied multi-parametric classification techniques such as Grey Theory **Grey Def** to not only detect abnormal behaviour but also to classify what type of attack is being attempted.

0.4.7 Network Again

Due to the previously stated marine effects on transmission, even assuming that existing trust structures could be deemed applicable to AUV operations, the metric-sets applied would have to be completely re-approached to take account of the unique communications environment. Normally, the types of metrics assessed involve packet loss rates, packet delay, and communications throughput, but additional physical layer metrics such as Received Signal Strength,and more behavioural metrics such as expected distance and deviations from expected motion paths, are being investigated to complement these MAC layer metrics.

The significant objects of work can be summarised as:

- **DC1** 1. An assessment of vulnerabilities to a fleet of AUVs during typical operations with an aim to develop a suitable threat model
- **DC2** 2. Identification of marine-specific metrics suitable to discriminate between legitimate and suspicious AUV behaviour.
- **DC3** 3. Development of a distributed trust management framework incorporating reputation analysis schemes throughout a fleet of AUVs
- **DC4** 4. And finally to explore and assess the feasibility of the framework for use across a range of operational tasks with an aim to integrate into existing frameworks such as MODAF/AGATE.

0.4.8 Pools

While the majority of the work is expected to be theoretical development and simulation of threat models, the facilities afforded by Professor Fontaine's CIIRF group at UPMC in France will provide access to real AUV systems. This experience is essential to determining real-world performance of different metric-sets, and to evaluate the

practicality of such schemes.

0.5 Project Structure

0.5.1 Team

Both supervisors have extensive experience in defence research, including research within the areas of Networking and AUV operations; Professor Marshall has been involved in the assessment, development and implementation of reliable and secure wireless networks for over 12 years, and Professor Fontaine is an established expert in the field of AUVs, including involvement with a number of NATO initiatives in this area, and has ties to research organisations such as the NATO Undersea Research Centre that will provide essential practical resources to this project.

Considering the potential exploitation of the project, both supervisors have experience in defence sponsored research and are aware of the relevant issues. Additionally both have extensive track records in international publication. Further, their associated institutions are already very well acquainted with commercialising research. For example, Prof Marshall has founded a successful wireless network security start-up which was spun-out from Queen's University. Queen's was also named the UK Entrepreneur University of the year for 2009. Professor Fontaine's involvement with NATO will also lead to further development of the resultant techniques and findings from this research, potentially leading to project-input to the forthcoming FP8 EU research call.

0.5.2 Project Monitoring

Beyond internal team monitoring, the monitoring structures in place within Queen's endeavour to keep PhD projects on track. Queen's institutes two major review points within the first year of the project, called the 'Three Month Report', and the Nine Month Differentiation.

Surprise Surprise, the Three Month Report is a report, delivered after three months of work, summarising the researchers progress, and including;

- Research Background and justifications
- Planned Research Objectives or key research questions (including justification on why these are important)
- A planned methodology including any ethical concerns or data-retention issues, as well as a general timetable

I'm currently in the process of drafting this report.

Six months later, there will a Differentiation report, mainly consisting of a significant review of key field literature, and a descriptive analysis of the intended methodology. Supplicant to this is a panel review. The panel then makes the recommendation whether my research is good enough to be classed at PhD level. Additionally, there is the option to 'retake' the differentiation. If necessary.

Beyond the initial year, there are annual reviews of ongoing research projects, and beyond Queen's, the expectation is that regular reviews will be undertaken with DSTL/DGA, although I hope that like this presentation; these reviews synchronise with Institution-mandated reviews so as to reduce my paperwork!

0.5.3 Defence Context

Moving on, the interest to defence for this project is clear; within DSTL's already stated areas of strategic importance, this research falls into at least four areas; namely Certification of Autonomous Systems; Shallow Oceanic Zone and Coastal Environment; Security and Vulnerability; as well as Human Operator Control of Unmanned Vehicles.

0.5.4 Defence Feedback

This work would provide the ability for a fleet of AUVs to operate over a much wider range of operations for much longer periods of time, in a much more secure and reliable state.

The self-detection and classification of abnormal behaviour within a fleet in the proposed distributed manner opens up the potential of a new range of secure and self-learning distributed intrusion detection systems, with potential applications both below and above the seas.

0.6 Cheers

Thank you for your time, and I'd be happy to answer any questions you might have.