Multi-Domain Trust Frameworks for Harsh Environments

Andrew Bolster
Department of Electrical Engineering and Electronics
University of Liverpool
Liverpool, UK
Email: bolster@liv.ac.uk

Alan Marshall
Department of Electrical Engineering and Electronics
University of Liverpool
Liverpool, UK
Email: alan.marshall@liv.ac.uk

***Abstract*—With the increasing application of autonomy in cyber-physical systems, Trust Management Frameworks (TMFs) are increasingly being applied to assist the efficiency, security, and reliability of decentralised and distributed autonomous systems, from highway-bound autonomous vehicles to aerial battlefield drones. Classical applications of trust management in Mobile Ad-Hoc Networks (MANETs) have focused solely on observations from the communications domain upon which to make trust assessments. However, these methods are not as effective in applications exhibiting sparse, delayed, or otherwise challenged communications environments. MD-TMF expands this paradigm to include relevant physical factors and movements to increase the threat area covered the trust framework. In this paper we demonstrate the use and operation of a multi-domain trust management framework (MD-TMF) for collaborative mobile autonomous networks (CMANs), using simulated underwater autonomous networks (UANs) as an exemplar application of a resource constrained, delay-tolerant, cyber-physical system. We also present a methodology for assessing the relative and collective performance of varying metrics in detection and differentiation of a range of communications and physical misbehaviours.**

I. Introduction

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Conclusion

The conclusion goes here.

Acknowledgment

The Authors would like to thank the DSTL/DGA UK/FR PhD Programme for their support during this project, as well as NATO CMRE for their advice and assistance.