Physical Behaviours for Trust Assessment in Autonomous Underwater MANETs

Pages: 9, Deadline: 25/3

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*—Relevant sections from the CFP art: Key Mgmt & Trust Establishment; Robotic Networks; Vehicular Networks & Protocols; Location Based Services; Mobility Managment**

Do this last

I. Introduction

Early attempts to secure and protect the integrity of Mobile Ad-hoc Networks have relied on some form of strong-cryptograpic methods to protect information being transited in routing packats. Such an approach does protect the integrity of individual pieces of data, the increased computation, and storage requirements of modern, strong, decentralised cryptography present a clear avenue for Denial of Service (DoS) attacks on MANET. This threat is particularly relevant in resource-constrained networks, where one or more aspects of the environment are limited, be it available power, locomotive mobility, data storage, onboard processing, available bandwidth, and channel resources such as capacity and delay. In such networks, where there is a requirement of security and/or integrity monitoring, strong-cryptographic methods present an entirely new threat-opportunity to potential attackers.

One solution to the trade-off between DoS-protection, and security is the establishment of assessment of "trustworthiness" of nodes within a local network. "Trust" in this case is an assessment of capability of a node based on previously observed behaviour. Using this Trust to make simple routing decisions is significantly faster that strong-cryptographic methods, particularly in multi-hhop networks or resource constrined networks[1].

With Trust being reliant on the near-real-time awareness of some behaviour, and Cryptography on the pre-establishment of some entropy store and the repeated reinforcement of that numerical security, they represent two very different approaches to security It is envisioned that going forward, some elements of both methodologies will be used in different contexts and applications.

However, these approaches to operational security have been totally focused on the establishment of trust/security in the communications domain, and ignore other potential threats to the network exploited through physical movement. This threat is particularly evident in collaborative autonomous systems where nodes are tasked to acccomplish some survey / exploration / observation objective in a distributed fashion, where individual nodes make decisions based on the actions of their "team". This collaboration opens the opportunity for a physically-misbehaving actor to selfishly conserve it's own resources, or maliciously "drain" a given target node. Current security / trust systems applied to MANETs are not concerned with the threat of such physical misbehaviours.

This paper proposes a new approach to trust in resource-constrained networks of autonomous systems based on their physical behaviour, assessing the viability of using the motion of nodes within a team to detect and potentially identify malicious or failing operation within a cohort. This is accomplished by looking specifically at operations within the three dimensions of the underwater space.

In the majority of Trusted autonomous mobile network implementations, a free space RF communications protocol such as 802.11 is used as the source of all information about the trustworthy operation of the network. Most current trust frameworks use a single type of observed communication action to derive trust assessments, typically successfully delivered or forwarded packets. By their nature, such implementations rely on relatively high bandwidth, low noise, low latency, and high channel occupancy where contention is tolerable. In contrast; in underwater environments, communications is sparse, delayful, noisy, and very prone to destructive contention. Therefore, observations of the communications processes used to assess trust occur much less frequently, with much greater error (noise) and delay than is experienced in terrestrial RF MANETS. In addition to the communications challenges, other considerations such as command and control isolation, as well as power and locomotive limitations, and the increasing drive towards the use of teams of smaller, cheaper, almost disposable autonomous underwater vehicles (AUVs), particularly in defense, ecological and petrochemical fields, present unique threats against trust management.

In Section II, we review the current use cases, deployments and mobility patterns of collaborative AUV operations, and the state-of-the-art in underwater localisation techniques. In Section III, we discuss the use of TMFs and their relevance and applicability to marine operations. In Section IV, we propose a collection of physical metrics to characterise the physical behaviours of node, and establish a set of physical "misbehaviours" to test these against. In Section V, we design a series of simulations, and tests to assess the detection and identification capabilities of three potential physical metrics for trust assessment.

II. AUV Mobility and Localisation

The use and applications of Autonomous Underwater Vehicles (AUVs) has undergone a great expansion in recent times; current applications and considerations are given below (summarised from [2]).

A. AUV operations and deployments

1) Hydrographic Survey: The use of AUVs in the place of manned-surface platforms or tethered undersea platforms enables greatly increased spatial and temporal sampling. Importantly, the separation of AUVs from the noisy sea surface enables much more efficient survey operations. This is particularly important when comparing to classical tow-line based measurements; where the mobility of the AUVs enables for much tighter-turning survey patterns or operation in inaccessible or hard-to-reach locations such as polar survey[**?**].

Another significant factor is cost; the daily cost of operating a manned vessel can be signficantly higher than the costs of deploying, operating and recovering one or more AUVs with equivalent capabilities[3]. Additionally, the use of low-power "glider" AUVs has lowered the barrier to entry for extended mission types, such as persistent environmental survey, or open-ocean operations. Depth-hardened AUVs have also opened up the deepest parts of the oceans to exploration, with the onboard autonomoy, imagery and Simultaneous Location and Mapping (SLAM) techniques allowing deep-dwelling survey AUVs to react to bottom-surface features without the need for a tight craft-to-surface control loop. The natural extension of these kind of applications is the use of AUVs on ice-covered planets such as Europa, where three-dimensional, autonomous navigation without an on-the-loop controller is vital for mission resource efficiency and success.

2) Hull and Infrastructure Inspection: Ongoing concerns regarding the security, safety and legality of international shipping has driven the application of AUVs to the area of near-surface hull and infrastructure inspections, looking for damage as well as devices such as limpet mines and other contraband. This use case puts a range of unique pressures on the AUV system; requiring highly accurate three-dimensional localisation and control to clearly image the contours of a hull[3]. Similarly, with the increasing use and criticality of intercontinental undersea optical fibre connections, using AUVs for both the laying of and inspection of these cables is an exciting area of work[**?**][**?**].

3) Marine Petrochemical: Oil and Gas industry requirements for high quality, low altitude bathymetry of seabed structures for infrastructure development (pipelines/drill platforms etc.) as well as monitoring of those structures over time (inspection etc.) is another significant application area, and a major driver of research investment. As in Hydrography, the mobility of AUVs is the biggest single advantage over classical platforms[**?**].

4) Military: Mine-Countermeasure Operations benefit greatly from, and significantly drive, AUV development; the ability to rapidly explore and covertly survey a potentially dangerous area without risking a human operator is a major benefit. This benefit applies to protection as well as incursion; the ability to have persistent survey of a valuable area such as a forward-operating harbour is increasingly essential, and as AUV technology, autonomy and security practices develop, this use is increasing. This Port Protection capability is particularly complex; teams of AUVs are expected to repeatedly survey an area and remain densly-connected enough to maintain end-to-end communications with all other nodes, in the face of an environment that is possibly not well surveyed initially, and includes dynamically moving obstacles (i.e. ships). In Sec. V, we use this Port Protection scenario as a baseline for our simplified simulation context.

Do I have to talk about the motion path?

For Chapter Look at redoing this with other mobilities (particularly distributed lawnmower)

B. Localisation Technologies

Given the subsurface nature of most AUV operations, terrestrial localisation techniques such as GPS are unavailable (below $\approx 20cm$ depth). However, a range of alternative techniques are used to maintain spacial awareness to a high degree of accuracy in the underwater environment.

1) Long baseline (LBL): Long-baseline localisation systems use a series of static surface/cable networked acoustic transponders to provide coordinated beacons and (usually) GPS-backed relative location information to local subsurface users. Such systems can be accurate to less that $0.1m$ or better in ideal deployments and are regularly used in controlled autonomous survey environments such as harbour patrol operations where the deployment area is bounded. However, the initial setup and deployment required in advance of any AUV operation makes LBL difficult to utilise in unbounded or contended areas. LBL systems can also be deployed on mobile surface platforms in the area (ships or buoys for example), but these applications put significant computational pressure on the end-point AUV and have greatly reduced accuracy compared to ideal deployments[4].

2) Doppler Velocity Log (DVL): Doppler logging involves the emission of directed acoustic "pings" that reflect off sea bed/surface interfaces that, when received back on the craft with multi-beam phased array acoustic transducers can measure both the absolute depth/altitude (z-axis) of the craft and through directional Doppler shifting, the relative (xy-translative) motion of the craft since the ping. While classical DVL was highly sensitive to shifting currents in the water column, advances in the development of Acoustic Doppler Current Profiling has turned that situation on it's head, enabling the compensation-for and measurement-of water currents down to the sub-meter level[5].

3) Inertial Navigation Systems (INS): Inertial navigation systems use gyroscopic procession to observe the relative acceleration of a mobile platform. This reference-relative monitoring is particularly useful in the underwater environment, as it detects the motion of AUVs as they are carried by the water itself. Bias Drift is a significant problem for INS systems operating over longer (hundreds of metres) distances, as they usually have some minimal amount of directional bias, that incurs a cumulative effect over time without assistance. Several sensor synthesis processes have been demonstrated which combine information from INS along with DVL data to improve localisation into the sub-decimeter level[2][6].

4) Simultaneous Location and Mapping (SLAM): Simultaneous Location and Mapping is the process of iteratively developing a feature-based model of an environment, and to use the relative movement within that modeled environment to obtain estimates of absolute positioning. SLAM has been most well developed in the contexts of either visual-based inspection using cameras, or LIDAR-style distance triangulation, however the same principles have been successfully applied using marine sonar readings, providing sub-meter accuracy, feature-relative localisation information that is (for the most part) environmentally agnostic[7].

III. Trust Management Frameworks

Trust Management Frameworks (TMFs) provide information to assist the estimation of future states and actions of nodes operating as teams, groups or networks. This information is used to optimize the performance of a team against malicious, selfish, or defective misbehaviour by one or more nodes. Previous research has established the advantages of implementing communications-based TMFs in terrestrial, 802.11 based MANETs, particularly in terms of preventing selfish operation in collaborative systems [8], and maintaining throughput in the presence of malicious actors [9]. These observations then inform future decisions of individual nodes, for example, route selection [10].

Recent work has demonstrated the use of a number of metrics to form a "vector" of trust. The Multi-parameter Trust Framework for MANETs (MTFM) [11], uses a range of communications metrics beyond packet delivery/loss rate (PLR) to assess trust. This vectorized trust also allows a system to detect and identify the tactics being used to undermine or subvert trust. This method as been previously applied to the marine space, comparing against a selection of existing communications TMFs [12] showing that MTFM is more effective at detecting misbehaviours in sparse communications environments.

Trust Management Frameworks (TMFs) are used to improve the efficiency, security, and reliability of decentralized and distributed autonomous systems. Techniques have been developed for high-speed, uncontended environments such as terrestrial 802.11 MANETs. However, these do not perform well in sparse / harsh environments such as those found in Underwater Acoustic Networks (UANs), where network nodes experience significant and variable delays, comparatively low data rates, large contention periods, and considerable multipath artefacts.[12]

Not sure how much detail to go into in this section; this paper isn't about the formation of trust from metrics, it's about the assessment of metrics at all

IV. Physical Behaviours for Trust

A. Physical Metrics

Three physical metrics are selected to encompass the relative distributions and activities of nodes within the network; Inter-node Distance Deviation (INDD), Inter-node Heading Deviation (INHD), and Node Speed. These metrics encapsulate the relative distributions of position and velocity of a particular observed node, optimising for the detection of outlying or deviant behaviour within the fleet.

Given that local nodes within the team are aware of the reported positions and velocities of their neighbours, it is believed that this is a reasonable initial set of metrics to establish the usefulness of physical metrics of trust assessment.

Additional metric constructions may be more suitable for certain contexts, platforms or operations, however these were selected in collaboration with UK DSTL and NATO CMRE as suitable, generic, assessments, viable on most current platforms in most current deployment schemes.

Conceptually, INDD is a measure of the average spacing of an observed node with respect to its neighbours. INHD is a similar approach with respect to node orientation.

As such, these metrics completly encapsulate and abstract the physical behaviour of any node, potentially performing any misbehaviour.

$$INDD_{i,j} = \frac{|P_j - \sum_x \frac{P_x}{N}|}{\frac{1}{N}\sum_x \sum_y |P_x - P_y| (\forall x \neq y)} \quad (1)$$

$$INHD_{i,j} = \hat{v} | v = V_j - \sum_x \frac{V_x}{N} \quad (2)$$

$$V_{i,j} = |V_j| \quad (3)$$

Where i and j are indices denoting the current observer node and the current observed node respectively; x is a summation index representing other nodes in the observers region of concern; Pj is the $[x, y, z]$ absolute position of the observed node (relative to some coordinated origin point agreed upon at launch) and Vj is the $[x, y, z]$ velocity of the observed node.

Thus, the metric vector used for the physical-trust assessment from one observer node to a given target node is;

$$X_{i,j} = \{\mathrm{INDD}_{i,j}, \mathrm{INHD}_{i,j}, , V_{i,j}\} \quad (4)$$

At each time-step, each node will have a separate X assessment vector for each node it has observed in that time. Ergo the fleet or team as a whole will have $N \times N$ assessment vectors at each timestep.

B. Physical Misbehaviours

Misbehaviours in the communications space is heavily investigated area in MANETs [13][14][15][16], but attacks and misbehaviours in the physical space are far less explored. Both in terrestrial and underwater contexts, as MANET applications expand and become increasingly *de rigueur*, the impacts of physical or operational misbehaviour become increasingly relevant. As in the communications space, the primary drivers of any "misbehaviour" come under two general categories; selfish operation or malicious subterfuge. Autonomous MANETs in general rely (or are at least, most effective) when all nodes operate fairly, be that in terms of their bandwidth sharing, energy usage, routing optimality or other factors. Physically, if a node is being "selfish", it may preferentially move to the edge of a network to minimise it's dynamic work allocation, or depending on it's intent, may insert itself into the centre of a network to maximise it's ability to capture, monitor, and manipulate traffic going across the network. In the context of a secure operation (or one that's assumed to be secure), the opportunity for capturing a legitimate node and replacing it with a modified clone. Assuming a highly capable outside actor and a multi-channel communications opportunity, there is even the possibility of a node appearing to "play along" with the crowd that occasionally breaks rank to route internal transmissions to a outside agent. In the underwater context this may mean an AUV following the rest of a team along a survey path and occasionally "breaking surface" to communicate to a malicious controller. Alternatively, if an inserted node is not totally aware of a given mission parameter, such as a particular survey or waypointing path, it may simply follow along, hoping not to be noticed.

In all these cases, such behaviour involves some element of behaving differently from the rest of the team, however, there are other cases where such individual "deviance" is observed; where a node is in some kind of mechanical "failure state". In the underwater context, this could be damage to the drive-train or navigation systems, causing it to lag behind or consistently drift off course. An ideal physical trust management system would be able to differentiate between both "malicious" behaviours and "failing" behaviours.

To investigate this hypothesis, we create two "bad" behaviours; one "malicious", where a cloned node is unaware of the missions' survey parameters and attempts to "hide" among the fleet, and a "failing" node, with an impaired drive train, increasing the drag force on the nodes movement. These two behaviours are designated *Shadow* and *SlowCoach* respectively.

V. Simulation and Validation

A. Simulation Background

Simulations were conducted using a Python based simulation framework, SimPy [17], with a network stack built upon AUVNetSim [18], with transmission parameters taken from and validated against [19] and [20]. For the purposes of this paper, this network is used for the dissemination of node location information, assuming suitable compression of internally assumed location data compressed into one 4096 bit acoustic data frame. Node kinematics are based on REMUS 100 Autonomous Underwater Vehicles, based on limits and core characteristics given in [21], [22] and [23]. For the purposes of this exploratory case we do not model the hydrodynamics of the control surfaces of the AUVs, however we do model axial drag as a resistive inertial force.

These limits are given in Table I

TABLE I
REMUS 100 Mobility Constraints as applied in simulation

Parameter	Unit	Value
Length	m	5.5
Diameter	m	0.5
Mass	kg	37
Max Speed	ms^{-1}	2.5
Cruising Speed	ms^{-1}	1.5
Max X-axis Turn	$^\circ s^{-1}$	4.5
Max Y-axis Turn	$^\circ s^{-1}$	4.5
Max Z-axis Turn	$^\circ s^{-1}$	4.5
Axial Drag Coefficient (c_d)	NA	3
Cross Section Area	m^2	0.13

B. Node Control Modelling

In our investigation, we use the example of a

Simple Boidean flocking [24] is used in addition to a cubic waypoint-survey behaviour to provide a collision-avoidance capability. This consists of three heuristic rules; Cohesion, Repulsion and Alignment, and are shown visually in 1 and mathematically below.

- Cohesion

$$F_{j,C} = F_A\left(p_j, \frac{1}{N}\sum_{\forall i\neq j}^{N} p_i, d_{max}\right) \tag{5}$$

- Repulsion

$$F_{j,R} = \sum_{\forall i\neq j}^{N} F_R\left(p_j, p_i, d_{max}\right)\big|d_{max} > \|p_i - p_j\|\big) \tag{6}$$

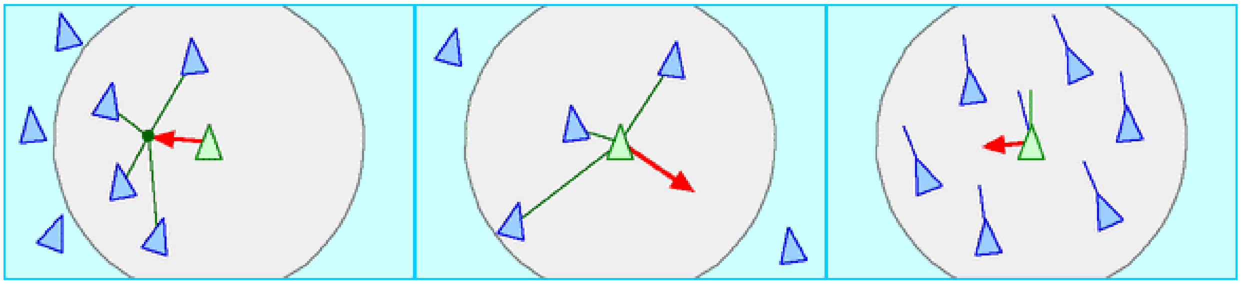
- Alignment

$$F_{j,CA} = \frac{1}{N}\cdot\left(\sum_{\forall i\neq j}^{N} \hat{v}_i\right) \tag{7}$$

where F's are force-vectors applied to the internal guidance of the AUV, Where F_A is a scaled vector attraction function, and F_R is an equivalent repulsion function

$$F_A(p^a, p^i) = (\widehat{p^a - p^i}) \times \frac{|p^a - p^i|}{d} \tag{8}$$

$$F_R(p^r, p^i) = (\widehat{p^i - p^r}) \times \frac{|p^r - p^i|}{d} \tag{9}$$



(a) Cohesion (b) Repulsion (c) Alignment

Fig. 1. Visual representation of the basic Boidean collision avoidance rules used

C. Standards of Accuracy

The key question of this paper is to assess the advantages and disadvantages of utilising trust from the physical domain.

It is important to clarify what is meant by "effective" in this case; the "effectiveness" of any trust assessment framework is taken as consisting of several parts.

1) the *accuracy* of detection and identification of a particular misbehaviour
2) the *timeliness* of such detections
3) the *complexity* of such analysis, including any specific training required
4) the *commonality* of the results of any detections between perspectives (also termed "isomorphism" of results)

In this case we are particularly interested in the accuracy of detection and identification of malicious / failing behaviours, and as such are looking at three key characteristics of accuracy; true detection accuracy (what percentage of "bad" behaviours are detected at all); false positive rates (what percentage of "control" behaviours are detected as being "bad"); and misidentification rates (how many instances of one bad behaviour are mischaracterised as the other and vie versa.

As such we have three primary questions to answer to establish if these metrics are useful:

- How accurate are these metrics in being able to easily differentiate between Normal and Abnormal behaviours in terms of True-Positive and False-Positive rates?
- What differentiation of response, if any, is there between the stated abnormal behaviours?
- Can a simple classification be built to characterise these differentiations of response, and what is it's True-Positive/False-Positive accuracy?

D. Analysis Workflow

Having established the metrics under investigation, $MANY$ simluation runs are executed for each scenario (i.e. one node "Maliciously" following the fleet with no mission information, one "Failing" node with simulated drivetrain issues, and one baseline control scenario where all nodes are behaving appropriatly. Eash of these simulated missions last for $duration$, matching realistic deployment times based on current MOD/NATO operations[25][**?**].

1) Metric Cleaning: In order to assess the viability of using the previously discussed metrics for behaviour assessment, the raw motion paths recorded by the simulation are fed into an analysis pipeline[1]. This pipeline initially

$$d_{i,j}^{m,t} = x_{i,j}^{m,t} - \frac{\sum_k x_{i,k}^{m,t}}{|M|} \tag{10}$$

$$\alpha_{i,j}^{m,t} = |\frac{d_{i,j}^{m,t}}{\sigma d_{i,j}^{m,t}}| \tag{11}$$

Where i and j are indices denoting the current observer node and the current observed node respectively; x is a summation index representing other nodes in the observers region of concern; X is the vector of metrics from 4; d is an intermediate value of the distance of a given observation from the mean, and α is a resulting normalised response value in terms of it's deviation from the mean.

2) Behaviour Detection and Classification:

This is going to be a bit of a black box while I work out what works automatically; previous versions simply looked at the "Highest Deviator", and while that still works in terms of detection, it's not massively useful in terms of Identification. Could be that in terms of the criteria posed above (simplicity of computation) that using the basic toolkits, we can't do it, however I'd rather not have every single paper I do in my career have half a page explaining the abstract operation of Gray Theory…

One simple behaviour detection is to apply Dixon's Q-test [26] to the resultant $\sum \alpha$ values for each node for each metric for each run a) establish if a "misbheaving node" exists in a given run, and b) identify that misbehaving node.

If you need padding at the end, explain Dixon

For our initial investigation we will use a Confidence Interval of 95%. Our initial hypothesis is that by using observations of the previously stated physical metrics, that we will be able to detect and identify misbehaviours. Within that context, this Confidence Interval indicates that we would expect only a 5%

[1] We do not currently deal with the case where nodes maliciously "fake" their location

chance that any run or node identified using the Q-test to *not* be a misbehaving run/node.

Further, due to the range of metrics available to us, by applying the Q-test on a per-metric basis, we can use the "votes" of each metric as a simplified consensus classifier.

There's got to be a better phrase than "consensus"...

This classifier may allow us to characterise some aspect of a given misbehaviour in terms of metrics it heavily impacts, and those that are less affected.

This can then be augmented by taking the residual deviation of $\sum \alpha_i$ to generate a "confidence" score of a given node being an outlier in a given metric;

$$C_i^m = \Sigma_t \sigma_i^m * \frac{N-1}{\sum_{x \neq i} \Sigma_t \sigma_x^m} \tag{12}$$

3) Operational Performance Metrics:

"How do we measure the impact of a bad-physical-behaviour on the operational success/efficiency of the fleet overall?". We have these numbers already in terms of energy use/efficiency of locomotion, cumulative distance covered, mean time to targets, etc, just need to wrap some words around it

VI. Results and Discussion

Fig. 2 shows the raw metric values (vertically) from one run of each behaviour (horizontally), starting with the Control case, where all node are behaving properly. The misbehaving node in the remaining cases. It clear that using the (unitless) INDD and INHD metrics, Alfa is the outlier and other, fairly behaving, nodes are all consistent in their metric values. This outlier-response is not nearly as clear in the Speed metric case (bottom row of Fig. 2).

In Fig. 3, where we have normalised the metric values as per (11), the outlying-characteristic of INHD and INDD is highlighted; largely eliminating the other nodes-responses. In the Speed response of Fig. 3, the Speed metric is not obviously highlighing any significant misbehaviours in that metric.

A. Detection of Misbehaviours

B. Identification of Misbehaviours

The below table is whats going to be used to condense all the ugly above into something processable across many runs (and most importatly, blind runs)

TABLE II
METRIC CONFIDENCE RESPONSES FOR KNOWN BEHAVIOURS (12)

metric var	INDD	INHD	Speed
Control	0.970	0.914	0.892
Shadow	4.459	3.875	1.797
SlowCoach	3.910	2.847	1.518
Tail	4.183	3.658	2.116

TABLE III
OVERALL Q-TEST OUTLIER DETECTION CHARACTERISTICS ACROSS 256 SIMULATIONS

Behaviour	Mean	Std
Shadow	0.979	0.144
SlowCoach	0.792	0.408
Tail	0.927	0.261
Waypoint	0.927	0.261

TABLE IV
PER-METRIC Q-TEST OUTLIER DETECTION CHARACTERISTICS ACROSS 256 SIMULATIONS

	Behaviour	INDD	INHD	Speed
mean	Shadow	1.000	1.000	0.938
	SlowCoach	1.000	1.000	0.375
	Tail	0.969	0.969	0.844
	Waypoint	0.875	0.938	0.969
std	Shadow	0.000	0.000	0.246
	SlowCoach	0.000	0.000	0.492
	Tail	0.177	0.177	0.369
	Waypoint	0.336	0.246	0.177

C. Impacts of Misbehaviour on operational performance

VII. Conclusion

In this paper we have demonstrated that with current and on-the-horizon underwater localisation techniques, that in certain mobility models, that a set of relatively simple geometric abstractions (INHD, INDD, and Speed), between nodes as part of an Underwater MANET can be used as a Trust Assessment and Establishment metric.

We show, using a basic cubic survey mobility model built upon a Boidian collision prevention behaviour that in a simulated underwater environment, the outputs of these metrics can be used to detect and differentiate between example malicious behaviour and potential failure states.

This verification further supports the assertions the authors have made previously in [27] that it is practical to extend Trust protocols such as Multi-parameter Trust Framework for MANETS (MTFM)[28] to include metrics and observations from the physical domain as well as those from the communication domain. This combination of physical and "logical" information would further support the decentralised and distributed establishment of observation based Trust, reducing the significant

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.

References

[1] J. Cordasco and S. Wetzel, "Cryptographic Versus Trust-based Methods for MANET Routing Security," *Electron. Notes Theor. Comput. Sci.*, vol. 197, no. 2, pp. 131–140, 2008.

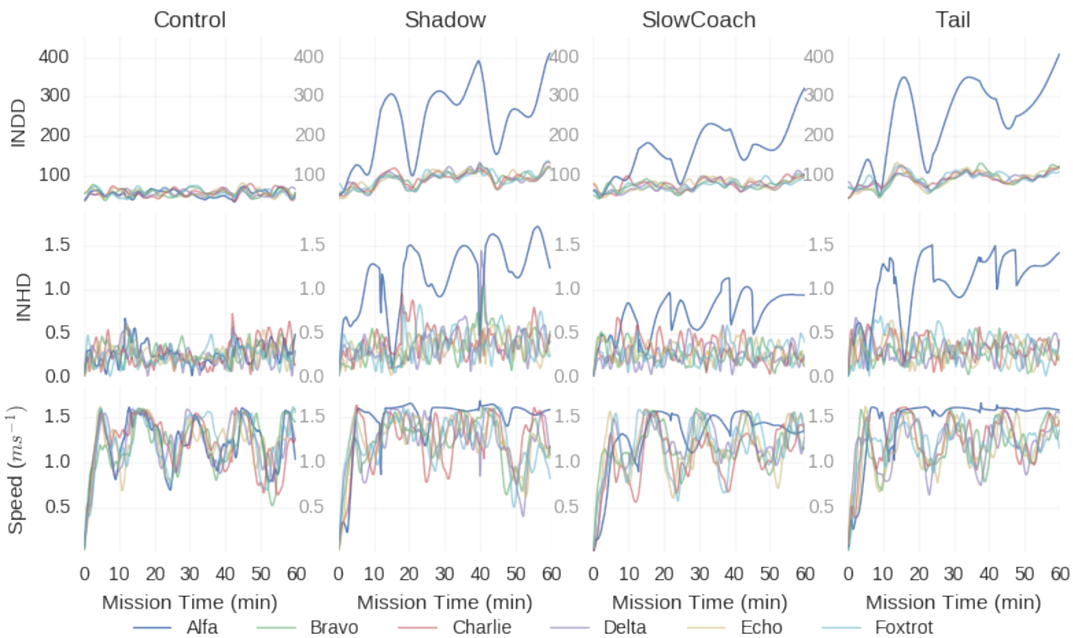


Fig. 2. Observed Metric Values for one simulation of each behaviour ($x_{i,j}^{m,t}$ from (10))

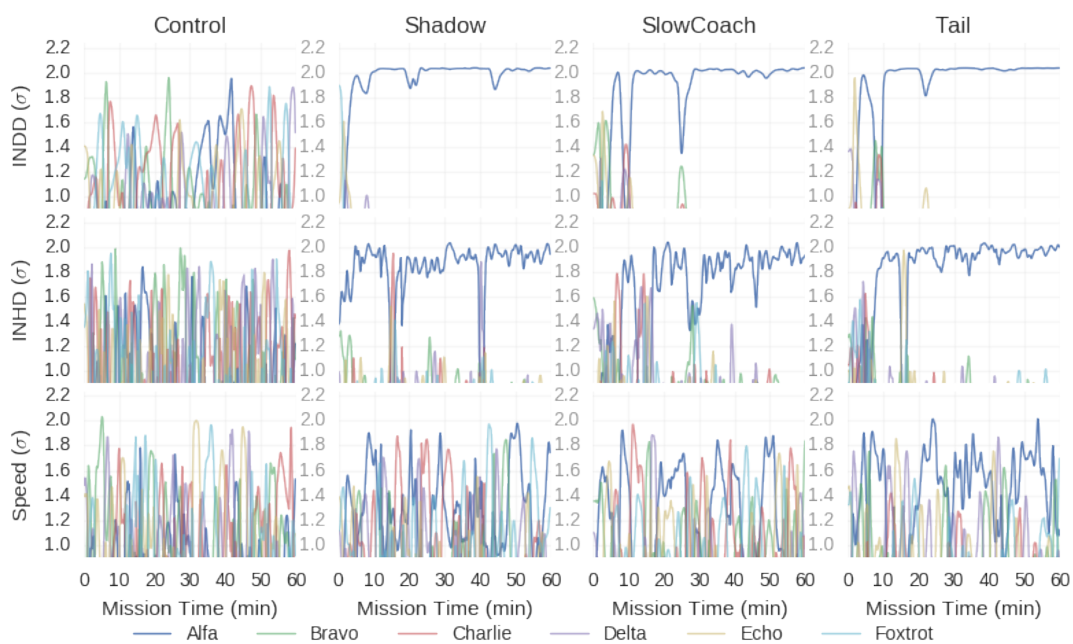
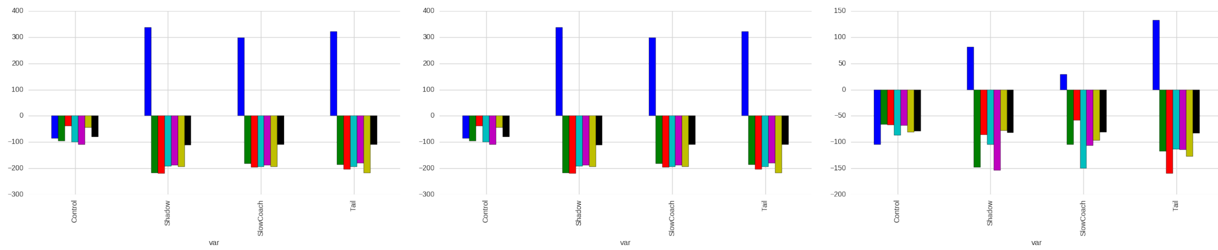


Fig. 3. Normalised Deviance values from one simulation of each behaviour ($\alpha_{i,j}^{m,t}$ from (11))



(a) INDD (b) INHD (c) Speed

Fig. 4. *VERY Draft; don't get pissy!*: Per-Node-Per-Run $\sum \alpha / T$

[2] B. Jalving, K. Gade, O. K. Hagen, and K. Vestgard, "A toolbox of aiding techniques for the HUGIN AUV integrated inertial navigation system," *Ocean. 2003. Proc.*, vol. 2, pp. 1146–1153 Vol.2, 2003.

[3] J. Nicholson and A. Healey, "Underwater Acoustic Communications and Networking: Recent Advances and Future Challenges," *Mar. Technol. Soc. J.*, vol. 42, no. 1, pp. 103–116, 2008. [Online]. Available: http://qub.library.ingentaconnect.com/content/mts/mtsj/2008/00000042/00000001/art00008

[4] a. Matos, N. Cruz, a. Martins, and F. L. Pereira, "Development and implementation of a low-cost LBL navigation system\nfor an AUV," *Ocean. '99. MTS/IEEE. Rid. Crest into 21st Century. Conf. Exhib. Conf. Proc. (IEEE Cat. No.99CH37008)*, vol. 2, pp. 774–779, 1999.

[5] J. Snyder, "Doppler Velocity Log (DVL) navigation for observation-class ROVs," *MTS/IEEE Seattle, Ocean. 2010*, no. Dvl, pp. 1–9, 2010.

[6] X. Liu, X. Xu, Y. Liu, and L. Wang, "Kalman filter for cross-noise in the integration of SINS and DVL," *Math. Probl. Eng.*, vol. 2014, no. Dvl, 2014.

[7] S. B. Williams, P. Newman, G. Dissanayake, and H. Durrant-Whyte, "Autonomous underwater simultaneous localisation and map building," *Robot. Autom. 2000. Proceedings. ICRA '00. IEEE Int. Conf.*, vol. 2, pp. 1793–1798, 2000.

[8] H. Li and M. Singhal, "Trust Management in Distributed Systems," *Computer (Long. Beach. Calif).*, vol. 40, no. 2, pp. 45–53, 2007. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622

[9] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol," in *Proc. 3rd ACM Int. Symp. Mob. ad hoc Netw. Comput. - MobiHoc '02*. ACM Press, 2002, pp. 226–236. [Online]. Available: http://dl.acm.org/citation.cfm?id=513800.513828

[10] J. Li, R. Li, J. Kato, J. Li, P. Liu, and H.-H. Chen, "Future Trust Management Framework for Mobile Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 108–114, apr 2007. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs{_}all.jsp?arnumber=4212452http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4481349

[11] J. Guo, A. Marshall, and B. Zhou, "A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks," *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*, pp. 142–149, 2011. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120813

[12] A. Bolster and A. Marshall, "Single and Multi-Metric Trust Management Frameworks for use in Underwater Autonomous Networks," in *Trust. 2015*, 2015.

[13] K. Konate and A. Gaye, "Attacks Analysis in Mobile Ad Hoc Networks: Modeling and Simulation," *2011 Second Int. Conf. Intell. Syst. Model. Simul.*, pp. 367–372, jan 2011. [Online]. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true{&}arnumber=5730376{&}contentType=Conference+Publications

[14] X. Wang, J. S. Wong, F. Stanley, and S. Basu, "Cross-Layer Based Anomaly Detection in Wireless Mesh Networks," *2009 Ninth Annu. Int. Symp. Appl. Internet*, pp. 9–15, jul 2009. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5230665

[15] I.-R. Chen, J. Guo, F. Bao, and J.-H. Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization," *Ad Hoc Networks*, vol. 19, pp. 59–74, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1570870514000419

[16] R. Mitchell, I.-r. Chen, and V. Tech, "A Survey of Intrusion Detection in Wireless Network Applications," 2014.

[17] K. Müller and T. Vignaux, "SimPy: Simulating Systems in Python," *ONLamp.com Python DevCenter*, feb 2003. [Online]. Available: http://www.onlamp.com/pub/a/python/2003/02/27/simpy.html?page=2

[18] J. Miquel and J. Montana, "AUVNetSim: A Simulator for Underwater Acoustic Networks," *Program*, pp. 1–13, 2008. [Online]. Available: http://users.ece.gatech.edu/jmjm3/publications/auvnetsim.pdf

[19] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," p. 34, 2007. [Online]. Available: http://www.mit.edu/{~}millitsa/resources/pdfs/bwdx.pdf

[20] A. Stefanov and M. Stojanovic, "Design and performance analysis of underwater acoustic networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 10, pp. 2012–2021, 2011.

[21] R. McEwen and K. Streitlien, "Modeling and control of a variable-length auv," *Proc 12th UUST*, pp. 1–42, 2006. [Online]. Available: http://www.mbari.org/staff/rob/uustrep.pdf

[22] J. Milgram, C. V. Alt, and T. Prestero, "Verification of a Six-Degree of Freedom Simulation Model for the REMUS Autonomous Underwater Vehicle by in partial fulfillment of the requirements for the degrees of and at the Chairperson , Committee on Graduate Students Verification of a Six-Degree of F," 2001.

[23] S. A. Samad, S. K. Shenoy, G. S. Kumar, and P. R. S. Pillai, "A Survey of Modeling and Simulation Tools for Underwater Acoustic Sensor Networks," *Networks*, pp. 40–47, 2011.

[24] C. W. Reynolds, "Boids (Flocks, Herds, and Schools: a Distributed Behavioral Model)," *SIGGRAPH 87 Proc. 14th Annu. Conf. Comput. Graph. Interact. Tech.*, vol. 21, no. 4, pp. 25–34, aug 1987. [Online]. Available: http://dl.acm.org/citation.cfm?id=37402.37406http://www.red3d.com/cwr/boids/

[25] A. Bolster, "Analysis of Trust Interfaces in Autonomous and Semi-Autonomous Collaborative MHPC Operations," The Technical Cooperation Program, Tech. Rep., 2014.

[26] R. B. Dean and W. J. Dixon, "Simplified Statistics for Small Numbers of Observations," *Anal. Chem.*, vol. 23, no. 4, pp. 636–638, 1951. [Online]. Available: http://pubs.acs.org/doi/abs/10.1021/ac60052a025

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

[28] J. Guo, "Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks," 2012.