Mobility 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**

I. Introduction

In the majority of Trusted autonomous mobile network implementations, a free space RF communications protocol such as 802.11 is used. By their nature, such implementations rely on relatively high bandwidth, low noise, low latency, high channel occupancy where contention is tolerable. In contrast; in underwater environments, communications is sparse, delayful, noisy, and very prone to destructive contention. Therefore the observations about the communications processes that are used to generate the trust metrics, 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, drive towards the use of teams of smaller, cheaper, almost disposable autonomous underwater vehicles (AUVs), particularly in defense, ecological and petrochemical fields. These increasingly decentralised applications present unique threats against trust management.

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 [1], and maintaining throughput in the presence of malicious actors [2]. Most current TMFs use a single type of observed communuication action to derive trust assessments, typically successfully delivered or forwarded packets. These observations then inform future decisions of individual nodes, for example, route selection [3].

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) [4], 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 [5] showing that MTFM is more effective at detecting misbehaviours in sparse communications environments.

This paper investigates the application of these communication-based Trust methodologies to the physical domain, to assess the viability of using the motion and mobility of nodes within a team to detect and potentially identify malicious or failing operation within a cohort. This is accomplised by looking specifically at operations within the three dimensions of the underwater space

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 in Table **??** (summarised from [6]). For the purposes of this exploratory case we do not model the hydrodynamics of the control surfaces of the AUVs.

TABLE I
REMUS 100 Mobility Constraints as applied in simulation

A. 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 in the underwater environment.

1) Long baseline (LBL): Long-baseline localisation systems use a series of 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 controled autonomous survey environments such as harbour patrol operations. LBL systems can also be relative to other mobile surface assets in the area (ships or buoys for example), but these applications put significant computational pressure on the end-point AUV[7].

2) Doppler Velocity Log (DVL): Doppler logging involves the emission of directed acoustic "pings" that reflect off sea bed/surface interfaces that, when recieved 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[8].

3) Inertial Navigation Systems (INS): Inertial nativation systems use gyoscopic 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 [6]

4) Simultaneous Location and Mapping (SLAM): [9]

Simple Boidean flocking [**?**] is used in addition to the guiding Waypointing behaviour to provide a collision-avoidance capability. This consists of three heuristic rules; Cohesion, Repulsion and Alignment, and are shown visually in **??** and mathematically below.

- Cohesion

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

- Repulsion

$$F_{j,R} = \sum_{\forall i\neq j}^{N} F_R\left(p_j, p_i, d_{max}\right)\big| d_{max} > \|p_i - p_j\|\big) \tag{2}$$

- Alignment

$$F_{j,CA} = \frac{1}{N}\cdot\left(\sum_{\forall i\neq j}^{N} \hat{v_i}\right) \tag{3}$$

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

III. Trust Management Frameworks

Trust Management Frameworks (TMFs) are being 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 multi-path artefacts.[5]

IV. Simulation Background

Simulations were conducted using a Python based simulation framework, SimPy [10], with a network stack built upon AUVNetSim [11], with transmission parameters (Table **??**) taken from and validated against [12] and [13]. For the purposes of this paper, this network is used for the disseminiation 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 [14], [15] and [16].

These limits are given in Table II

TABLE II
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

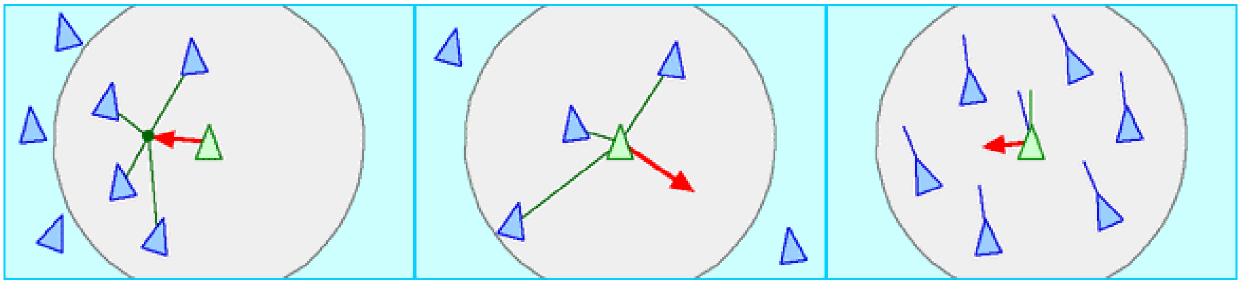
A. Standards of Accuracy

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.



(a) Cohesion

(b) Repulsion

(c) Alignment

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

B. 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.

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.

$$INDD_{i,j} = \frac{|P_j - \sum_x \frac{P_x}{N}|}{\frac{1}{N}\sum_x \sum_y |P_x - P_y| (\forall x \neq y)} \tag{4}$$

$$INHD_{i,j} = \hat{v} | v = V_j - \sum_x \frac{V_x}{N} \tag{5}$$

$$V_{i,j} = |V_j| \tag{6}$$

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;

$$X_{i,j} = \{\text{INDD}_{i,j}, \text{INHD}_{i,j},, V_{i,j}\} \tag{7}$$

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.

C. Physical Misbehaviours

Misbehaviours in the communications space is heavily investigated area in MANETs [17][18][19][20], 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 drivetrain 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.

```
for all m in M do
    for all t do
        $d_{i,j}^{m,t} = x_{i,j}^{m,t} - \frac{\sum_k x_{i,k}^{m,t}}{|M|}$
        $\alpha_{i,j}^{m,t} = |\frac{d_{i,j}^{m,t}}{\sigma d_{i,j}^{m,t}}|$
    end for
end for
```

These two behaviours are designated *Shadow* and *SlowCoach* respectively.

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[21][**?**].

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

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 **??**; d is an intermediate value of the deviation of a given observation from the mean, and α is a resulting

E. Impacts of behaviour on fleet performance

V. 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 [22] that it is practical to extend Trust protocols such as Multi-parameter Trust Framework for MANETS (MTFM)[23] 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

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

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] 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

[2] 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

[3] 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

[4] 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

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

[6] 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.

[7] 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.

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

[9] 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 vol.2, 2000.

[10] 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

[11] 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

[12] 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

[13] 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.

[14] 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

[15] 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.

[16] 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.

[17] 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

[18] 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

[19] 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

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

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

[22] 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/

[23] 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

[24] J. Guo, “Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks,” 2012.