Analytical Metric Weight Generation for Multi-Domain Trust in Autonomous Underwater MANETs

Andrew Bolster and Alan Marshall

University of Liverpool

{andrew.bolster,alan.marshall}@liv.ac.uk

UComms 2016, Lerici, Italy

Ieri

Physical Characterisation of Acomms Media, Channel Access Strategies, Centralised Routing Topologies

Oggi

Collaborative access control, Untethered operations, MIMO, (some) Networking Abstractions, Experimental Autonomy, DLL interface standardisation, static-site as a Service (LOON)

Domani

Decentralised local resource coordination, Reactive/Application driven Autonomy, Generalised IP-like abstractions, AUV as a Service?

Ieri, oggi, domani

Ieri

Physical Characterisation of Acomms Media, Channel Access Strategies, Centralised Routing Topologies

Oggi

Collaborative access control, Untethered operations, MIMO, (some) Networking Abstractions, Experimental Autonomy, DLL interface standardisation, static-site as a Service (LOON)

Domani

Decentralised local resource coordination, Reactive/Application driven Autonomy, Generalised IP-like abstractions, AUV as a Service?

I hope you guys get this stuff right otherwise I'm stuffed.

Outline

Trust

"the level of confidence one agent has in another to perform a given action on request or in a certain context"

Trust

"the level of confidence one agent has in another to perform a given action on request or in a certain context"

Usefulness of Trust in Autonomy

- Trust vs Security?

Usefulness of Trust in Autonomy

- Trust vs Security?
- Trust vs Autonomy?

Usefulness of Trust in Autonomy

- Trust vs Security?
- Trust vs Autonomy?
- Trust vs Formal Verification

Trust Modeling

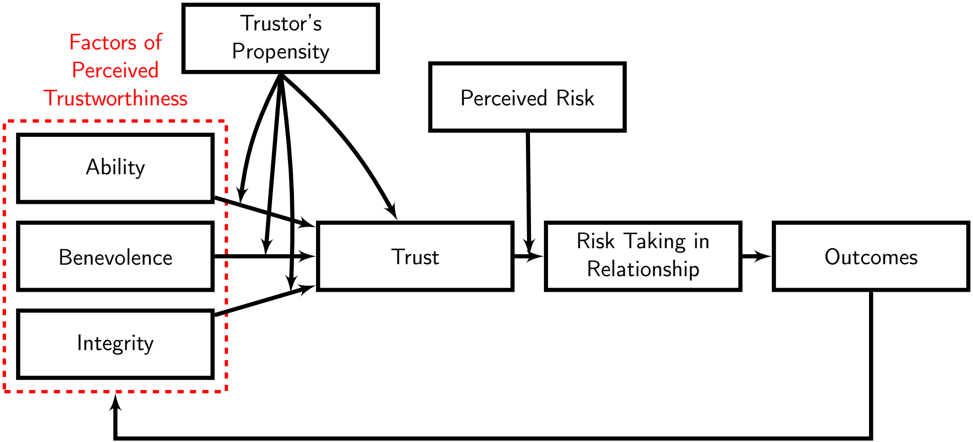


Fig. 1: Model of Trust (from Mayer, Davis, and Schoorman [1])

Context

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.
- What metrics are suitable for use underwater?
- How do MANET Single and Multi-Metric Frameworks perform in UWA?[3]

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.
- What metrics are suitable for use underwater?
- How do MANET Single and Multi-Metric Frameworks perform in UWA?[3]
  badly

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.
- What metrics are suitable for use underwater?
- How do MANET Single and Multi-Metric Frameworks perform in UWA?[3]
  badly, but multi can just about survive

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.
- What metrics are suitable for use underwater?
- How do MANET Single and Multi-Metric Frameworks perform in UWA?[3]
  badly, but multi can just about survive
- How to robustly optimise multi-metric/domain abstraction?

Context

- Trust is useful in Ad-hoc/distributed/decentralised nets
- Trust Management Frameworks (TMFs) require reassessment in UWA
- Most rely on one type of observation (metric) (PLR)
- Recent work[2] fuses multiple metrics for assessment.
- What metrics are suitable for use underwater?
- How do MANET Single and Multi-Metric Frameworks perform in UWA?[3]
  badly, but multi can just about survive
- How to robustly optimise multi-metric/domain abstraction? and is it worthwhile?

Outline

Trust in Conventional RF MANETS

- TMFs provide information to assist the estimation of future states and actions of nodes within networks.
- Centralised methods unsuitable for dynamic networks in terms of efficiency and robustness.[4]
- Need to detect, identify, & mitigate threats in a distributed fashion.

Single-Metric TMFs

Most can be generalised as single-value estimations of PLR/Successful Routes, with the incorporation of some *meta*-observations e.g. Topology

- *Hermes*[5] - Bayesian estimation based on PLR
- *OTMF*[6] - Collaborative Bayesian Trust
- *TSR*[7] - HMM route assessment, Session Loss Rate.
- *CONFIDANT*[8] - Probabilistic PLR assessment, inc. topology & reputation weighting.
- *Fuzzy Trust-Based Filtering*[9] - Fuzzy classification of packet delivery

Single-Metric TMFs

- Opportunities for malicious actors to undermine the operation of a network.
- Not an issue in networks where Comms. is the primary operating concern, but is significant in resource constrained environments

Single-Metric TMFs

- Opportunities for malicious actors to undermine the operation of a network.
- Not an issue in networks where Comms. is the primary operating concern, but is significant in resource constrained environments like UWA

Multi-Metric TMF

Multi-metric Trust For MANETS (MTFM)[2]

- Additional metrics as well as PLR,
- Topological relationship,
- Metric weighting enables behaviour classification
- Grey Relational Grading
  - dynamic runtime normalisation, assessing comparative trust within a cohort of actors.

Multi-Metric TMF

Multi-metric Trust For MANETS (MTFM)[2]

- Additional metrics as well as PLR,
- Topological relationship,
- Metric weighting enables behaviour classification
- Grey Relational Grading
    - dynamic runtime normalisation, assessing comparative trust within a cohort of actors.

Operates favourably in RF against OTMF and Hermes, accurately detecting, identifying, & characterising misbehaviours.[2]

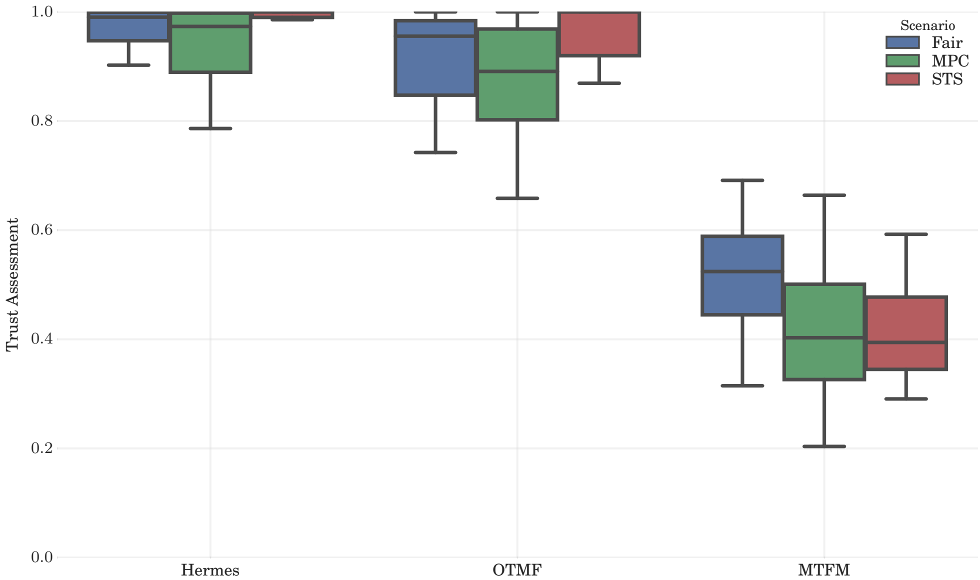
Multi-Metric TMF

Multi-metric Trust For MANETS (MTFM)[2]

- Additional metrics as well as PLR,
- Topological relationship,
- Metric weighting enables behaviour classification
- Grey Relational Grading
  - dynamic runtime normalisation, assessing comparative trust within a cohort of actors.

Operates favourably in RF against OTMF and Hermes, accurately detecting, identifying, & characterising misbehaviours.[2] Turns out it is "not as bad as the rest" in UWAN.[3]

Multi-Metrics Comms TMF performance



Outline

- Background
- Motivation
  - Trust
  - Related Work
  - Challenges to Trust in Underwater Networks
- Our Contribution
  - Multi-Metric Trust Assessment
  - Experimental Context
  - Metric Significance

Operational Considerations: Collaborative AUV Survey

Context:

- Fleets of up to 16 collaborating Autonomous Underwater Vehicles(AUVs) (not "Swarms")
- Constrained in Power, Mobility, Processing, Storage Capacity
- Tasked to perform ongoing survey of an area

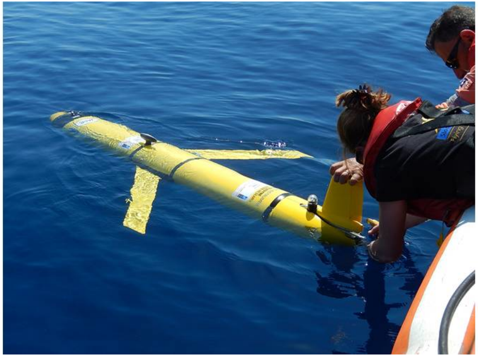


Fig. 2: REMUS 100 AUV as deployed at NATO CMRE La Spezia

Operational Considerations: Collaborative AUV Survey

Context:

- Fleets of up to 16 collaborating Autonomous Underwater Vehicles(AUVs) (not “Swarms”)
- Constrained in Power, Mobility, Processing, Storage Capacity
- Tasked to perform ongoing survey of an area

Communications Efficiency is not the only factor at risk from malicious exploitation

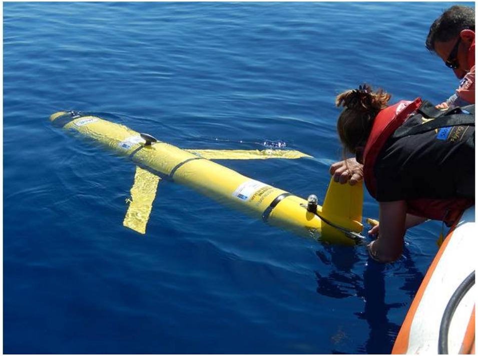


Fig. 2: REMUS 100 AUV as deployed at NATO CMRE La Spezia

Threat Surface

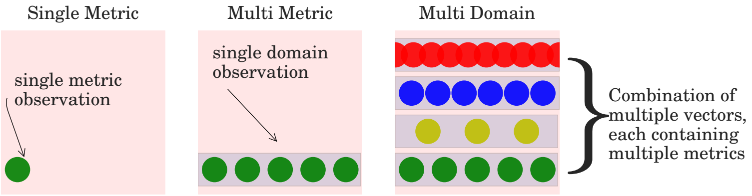


Fig. 3: Multi-Domain Threat Surface

Threat Surface

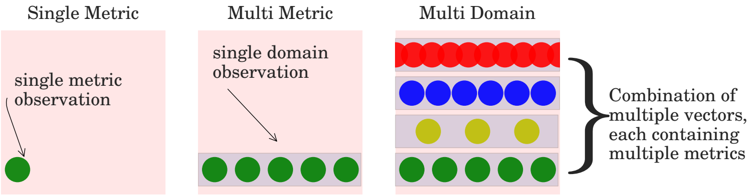


Fig. 3: Multi-Domain Threat Surface

Current trust methods monitor a tiny area of the potential threat surface

Outline

Multi-Metric Weighted Trust with Grey relations

$$\theta_{k,j}^{t} = \frac{\min_k |a_{k,j}^{t} - g_j^t| + \rho \max_k |a_{k,j}^{t} - g_j^t|}{|a_{k,j}^{t} - g_j^t| + \rho \max_k |a_{k,j}^{t} - g_j^t|} \tag{1}$$

$$\phi_{k,j}^{t} = \frac{\min_k |a_{k,j}^{t} - b_j^t| + \rho \max_k |a_{k,j}^{t} - b_j^t|}{|a_{k,j}^{t} - b_j^t| + \rho \max_k |a_{k,j}^{t} - b_j^t|} \tag{2}$$

$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t\right] \tag{3}$$

$$T_k^t = (1 + (\phi_k^t)^2 / (\theta_k^t)^2)^{-1} \tag{4}$$

Where $a_{k,j}^t$ is the value of an observed metric x_j for a given node k at time t, g and b are respectively the "good" and "bad" reference metric sequences from $\{a_{k,j}^t k = 1, 2 \ldots K\}$, $H = [h_0 \ldots h_M]$ is a metric weighting vector such that $\sum h_j = 1$

Factor of Opportunity in Trust Assessment

Weight

$H = [h_j \forall j in [0 \cdots M]]$

Relative importance of a given metric j

Valence

$g_j \mapsto max, b_j \mapsto min$ VS $g_j \mapsto min, b_j \mapsto max$

Is this metric j positively or negatively related to Trust?

Optimisation vector of Trust assessment

Trust assessment of misbehaving node should be:

1. maximally deviant wrt. “fair” nodes
2. identified as “low”

Optimisation vector of Trust assessment

Trust assessment of misbehaving node should be:

1. maximally deviant wrt. "fair" nodes
2. identified as "low"

Objective Functions

$$\Delta T_{ix} = \frac{\sum_{j \neq x} \left(\overline{T_{i,j}}^{\forall t} \right)}{N-1} - \overline{T_{i,x}}^{\forall t} \tag{5}$$

$$\Delta T_{ix}^{-} = \frac{\sum_{j \neq x} \Delta T_{ij}}{N-1} - \overline{\Delta T_{i,x}}^{\forall t} \tag{6}$$

Proposed General Methodology

Assess the relative importance of metrics in differentiating between behaviours using Random Forest Ensemble regression.
Constrained iterative solution space for valence enumeration.

Metric Domains

Communications

$$X_{comms} = \{D, P_{RX}, P_{TX}, S, G, PLR\} \tag{7}$$

Metric Domains

Communications

$$X_{comms} = \{D, P_{RX}, P_{TX}, S, G, PLR\} \tag{7}$$

Physical

$$INDD_{i,j} = \frac{|P_j - \sum_x \frac{P_x}{N}|}{\frac{1}{N}\sum_x \sum_y |P_x - P_y|(\forall x \neq y)} \tag{8}$$

$$INHD_{i,j} = \hat{v}|v = V_j - \sum_x \frac{V_x}{N} \tag{9}$$

$$V_{i,j} = |V_j| \tag{10}$$

$$X_{phy} = \{\mathrm{INDD}, \mathrm{INHD}, V\} \tag{11}$$

Multi-domain Metric Vector

Simplest possible combination; vector concatenation across domains

$$\begin{aligned} X_{merge} &= (X_{comms}|X_{phy}) \\ &= \{D, P_{RX}, P_{TX}, S, G, PLR, \mathrm{INDD}, \mathrm{INHD}, V\} \end{aligned} \tag{12}$$

Multi-domain Metric Vector

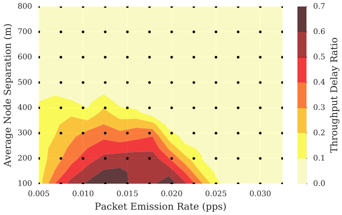
Simplest possible combination; vector concatenation across domains

$$X_{merge} = (X_{comms} | X_{phy}) = \{D, P_{RX}, P_{TX}, S, G, PLR, \mathrm{INDD}, \mathrm{INHD}, V\} \tag{12}$$

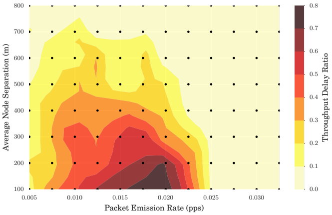
Not all metrics created equally
(or equally relevant to specific behaviours)

Outline

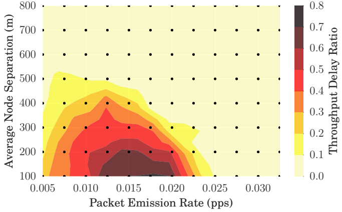
Scaling Considerations



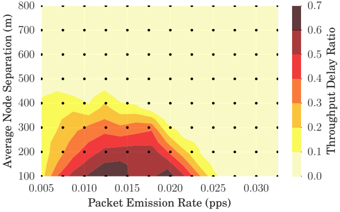
(a) All Nodes Static



(b) n_1 Random Walk



(c) All nodes but n_1 Random Walk



(d) All nodes Random Walk

Misbehaviour Specification

Assumptions

- Consistent misbehaviour
- Single misbehaver
- Honest position reporting (/Collaborative Localisation?)

Misbehaviours of n_a

- *Malicious Power Control*(MPC) - attacker makes n_t appear selfish by ++ power $n_i \forall i \neq t$
- *Selfish Target Selection*(STS) - node preferentially communicates with nodes close to it.
- *Shadowing* - follows with no mission knowledge.
- *SlowCoach* - 'misbehaver' with simulated prop. fouling

Base Behaviour: Port protection pattern with dynamic Boidean collision

Scaling Considerations

- Simulations based on SimPy,[10] Network stack using AUVNetSim[11] and channel constraints based on Stojaovic and Stefanov[12,13] ▸ Details

Scaling Considerations

- Simulations based on SimPy,[10] Network stack using AUVNetSim[11] and channel constraints based on Stojaovic and Stefanov[12,13] ▸ Details
- Established a safe operating zone optimising for delay/throughput ▸ Details
- Six per-link communications metrics

Scaling Considerations

- Simulations based on SimPy,[10] Network stack using AUVNetSim[11] and channel constraints based on Stojaovic and Stefanov[12,13] Details
- Established a safe operating zone optimising for delay/throughput Details
- Six per-link communications metrics

- Received Power
- Received Throughput
- E2E Delay
- Transmitted Power
- Transmitted Throughput
- Packet Loss Rate

Outline

Regression of Metric Significance

Aim: Establish which metrics are important in discriminating behaviours

Regression of Metric Significance

Aim: Establish which metrics are important in discriminating behaviours

- Distributed Random Forest Regression[14]
- 18661 Metric Weight Vectors ($H(X_{\text{merge}})$), 512 random trees
- 16 Random starts of each of the 4 misbehaving scenarios for 6 nodes for 6 hour "missions"
- 32 Random starts of each of the "fair" mission
- Regression identifies the significance of metrics in classifying between the possible behaviours + "fair"

Metric Significance

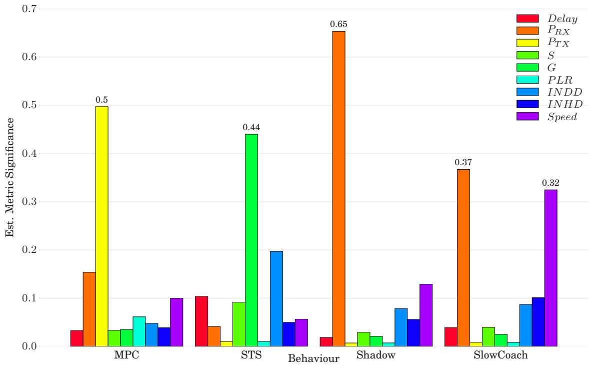


Fig. 4: Multi Domain Metric Features (X_{merge})

Metric Significance

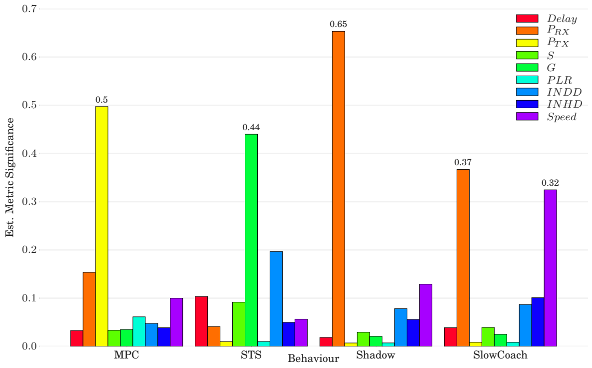


Fig. 4: Multi Domain Metric Features (X_{merge})

Brute force valence search with $R > 0.1 \mapsto$ massive reduction in complexity space

Also apply to specific domains for comparison

i.e. $X_{\text{comms}}, X_{\text{phys}}$

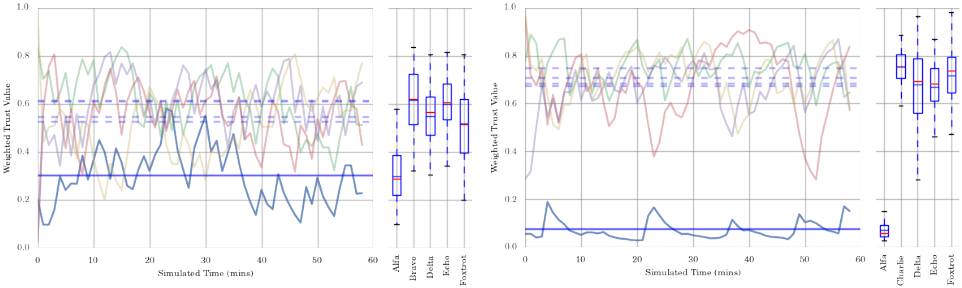
Also apply to specific domains for comparison

i.e. $X_{\text{comms}}, X_{\text{phys}}$

Table 1: ΔT across domains and detected behaviours

Domain	Behaviour				Avg.
	MPC	STS	Shadow	SlowCoach	
X_{merge}	0.90	0.10	0.50	0.63	0.53
X_{comms}	0.95	0.17	0.28	0.27	0.42
X_{phys}	0.02	0.02	0.43	0.76	0.31
Avg.	0.67	0.10	0.41	0.56	0.44

That's nice but what does it mean?

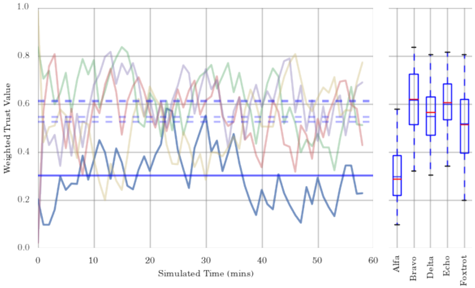


(a) Comms. Metric Trust Response

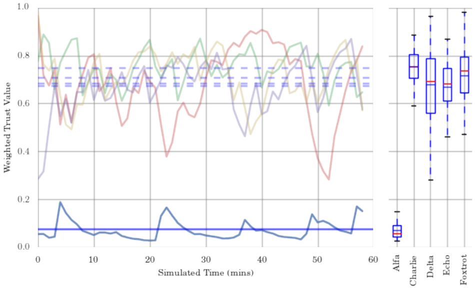
(b) Full Metric Trust Response

Fig. 5: Trust Responses for SlowCoach using domain-optimised weights

That's nice but what does it mean?



(a) Comms. Metric Trust Response



(b) Full Metric Trust Response

Fig. 5: Trust Responses for SlowCoach using domain-optimised weights

Misbehaviours are more eaily descernible when weighted

FYI Detection Characteristics

Domain	True Positive Identification of Misbehaver				False Positive Identification of Misbehaver			
	MPC	STS	Shadow	SlowCoach	MPC	STS	Shadow	SlowCoach
Full	1.00	0.03	0.63	0.98	0.00	0.07	0.00	0.0
Comms	1.00	0.05	0.18	0.39	0.00	0.03	0.04	0.0
Phys	0.03	0.02	0.40	0.85	0.12	0.09	0.00	0.0

More stuff not in the paper but FYI

Are our domain assumptions useful? Are there better ways to group metrics/behaviours?

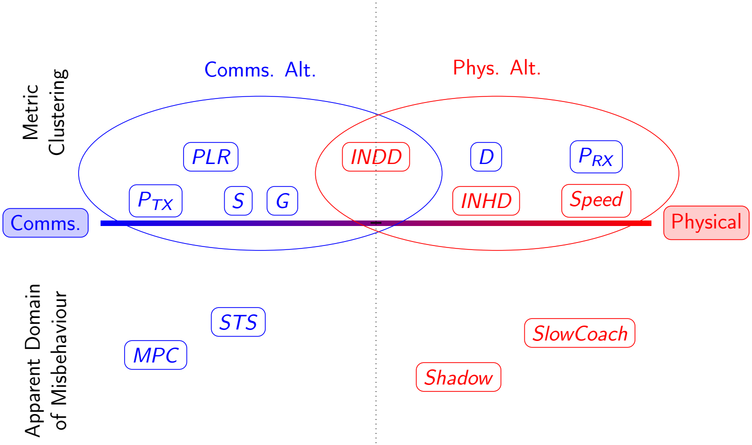
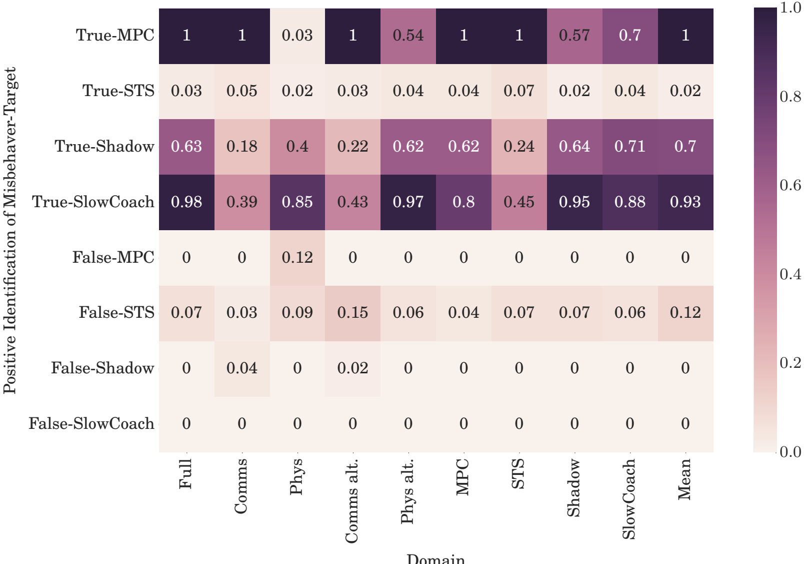


Fig. 6: Possible Alternate Metric Domain Groupings?

What about going to extremes?



Key Observations

- PLR not the most useful metric in discriminating behaviours

Key Observations

- PLR not the most useful metric in discriminating behaviours
- Combination of Significance and Correlations provide selectivity

Key Observations

- PLR not the most useful metric in discriminating behaviours
- Combination of Significance and Correlations provide selectivity
- MTFM has capability to finely discriminate between similar misbehaviours

Key Observations

- PLR not the most useful metric in discriminating behaviours
- Combination of Significance and Correlations provide selectivity
- MTFM has capability to finely discriminate between similar misbehaviours
- Identifying this classification "comb" is computationally intensive and grows exponentially with number of metrics involved for brute force regression

Key Observations

- PLR not the most useful metric in discriminating behaviours
- Combination of Significance and Correlations provide selectivity
- MTFM has capability to finely discriminate between similar misbehaviours
- Identifying this classification "comb" is computationally intensive and grows exponentially with number of metrics involved for brute force regression
- Use of Ensemble ML method and relevance filtering = Practical Real-time training

Key Observations

- PLR not the most useful metric in discriminating behaviours
- Combination of Significance and Correlations provide selectivity
- MTFM has capability to finely discriminate between similar misbehaviours
- Identifying this classification "comb" is computationally intensive and grows exponentially with number of metrics involved for brute force regression
- Use of Ensemble ML method and relevance filtering = Practical Real-time training
- High simulated selectivity depending on behaviour class

Done

Δ

- UWA Multi Metric Comms Trust
- Detection of non-comms misbehaviours/fouling even just using comms metrics
- Methodology for exploring / training / metric relevance
- Minimal performance specification

Σ

- UWA Trust is Hard & it's mostly the channels' fault
- Single-Metric Trust is unstable in such an environments
- Multi-Metric Trust works & can discriminate behaviours
- Not all metrics are equally useful
- Simple classifiers can be V good in some behaviours

Left/Next

$\notin$

- Smarter Detection Classifier
- Cooperative / Periodic / Variable attack profiles
- Commonality of detection filters across Multiple-base scenarios
- Heterogenous Node capabilities

Left/Next

$\notin$

- Smarter Detection Classifier
- Cooperative / Periodic / Variable attack profiles
- Commonality of detection filters across Multiple-base scenarios
- Heterogenous Node capabilities
- Real experiments and Cross sim-implementations

Left/Next

$\notin$

- Smarter Detection Classifier
- Cooperative / Periodic / Variable attack profiles
- Commonality of detection filters across Multiple-base scenarios
- Heterogenous Node capabilities
- Real experiments and Cross sim-implementations

$\mathbb{E}$

- Network that works
- Stable Abstractions / Interoperability
- reflective autonomy

References I

Roger C Mayer, James H Davis, and F David Schoorman. "An Integrative Model of Organizational Trust". In: *Acad. Manag. Rev.* 20.3 (July 1995), pp. 709–734. ISSN: 03637425. DOI: 10.2307/258792. URL: http://www.jstor.org/stable/258792.

Ji Guo, Alan Marshall, and Bosheng Zhou. "A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks". In: *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* (2011), pp. 142–149. DOI: 10.1109/TrustCom.2011.21. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120813.

References II

Andrew Bolster and Alan Marshall. "Single and Multi-metric Trust Management Frameworks for Use in Underwater Autonomous Networks". In: *Trust. 2015 IEEE*. Vol. 1. Aug. 2015, pp. 685–693. DOI: 10.1109/Trustcom.2015.435. URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=7345343.

Andrea Caiti. "Cooperative distributed behaviours of an AUV network for asset protection with communication constraints". In: *Ocean. 2011 IEEE-Spain* (2011). URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=6003463.

Charikleia Zouridaki et al. "A quantitative trust establishment framework for reliable data packet delivery in MANETs". In: *Proc. 3rd ACM Work. Secur. ad hoc Sens. networks* (2005), pp. 1–10. ISSN: 0926227X. DOI: 10.1145/1102219.1102222.

References III

Jie Li et al. "Future Trust Management Framework for Mobile Ad Hoc Networks". In: *IEEE Commun. Mag.* 46.4 (Apr. 2007), pp. 108–114. ISSN: 01636804. DOI: 10.1109/MCOM.2008.4481349. URL: http://ieeexplore.ieee.org/xpls/abs%7B%5C_%7Dall.jsp?arnumber=4212452%20http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4481349.

MEG E G Moe, BE E Helvik, and SJ J Knapskog. "TSR: Trust-based secure MANET routing using HMMs". In: *...symposium QoS Secur. ...* (2008), pp. 83–90. URL: http://dl.acm.org/citation.cfm?id=1454602.

- Sonja Buchegger and Jean-Yves 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. ISBN: 1581135017. DOI: 10.1145/513800.513828. URL: http://dl.acm.org/citation.cfm?id=513800.513828.
- Junhai Luo et al. "Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks". In: *2008 33rd IEEE Conf. Local Comput. Networks* (2008), pp. 305–311. DOI: 10.1109/LCN.2008.4664184. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4664184.
- Klaus Müller and Tony Vignaux. "SimPy: Simulating Systems in Python". In: *ONLamp.com Python DevCenter* (Feb. 2003). URL: http://www.onlamp.com/pub/a/python/2003/02/27/simpy.html?page=2.

References V

Josep Miquel and Jornet Montana. "AUVNetSim: A Simulator for Underwater Acoustic Networks". In: *Program* (2008), pp. 1–13. URL: http://users.ece.gatech.edu/jmjm3/publications/auvnetsim.pdf.

Milica Stojanovic. *On the relationship between capacity and distance in an underwater acoustic communication channel.* 2007. DOI: 10.1145/1347364.1347373. URL: http://www.mit.edu/%7B~%7Dmillitsa/resources/pdfs/bwdx.pdf.

Andrej Stefanov and Milica Stojanovic. "Design and performance analysis of underwater acoustic networks". In: *IEEE J. Sel. Areas Commun.* 29.10 (2011), pp. 2012–2021. ISSN: 07338716. DOI: 10.1109/JSAC.2011.111211.

References VI

L Breiman. “Random forests”. In: *Mach. Learn.* (2001), pp. 5–32. ISSN: 0885-6125. DOI: 10.1023/A:1010933404324. arXiv: /dx.doi.org/10.1023{\%}2FA{\%}3A1010933404324 [http:]. URL: http://link.springer.com/article/10.1023/A:1010933404324.

Jim Partan, Jim Kurose, and Brian Neil Levine. “A survey of practical issues in underwater networks”. In: *Proc. 1st ACM Int. Work. Underw. networks WUWNet 06* 11.4 (2006), p. 17. ISSN: 15591662. DOI: 10.1145/1161039.1161045. URL: http://portal.acm.org/citation.cfm?doid=1161039.1161045.

Thank You / QnA?

Say Hello!

- bolster@liv.ac.uk
- me@bolster.online
- @bolster
- bolster.online
- andrewbolster
- "Andrew Bolster"
- bolster

Communications Channel Considerations

Key Characteristics of the Marine Acoustic Channel:[**Urick1983a**, 15,12,13]

- Slow propagation ($1400ms^{-1}$) incurring long delays
- Inter-symbol interference
- Doppler Spreading
- Non-Linear propagation due to refraction
- Fast & Slow fades from environmental factors (flora/fauna/surface and seabed conditions)
- Freq. dependant attenuation
- Significant destructive multipath effects

Attenuation in the Marine Acoustic Channel

The attenuation that occurs in an underwater acoustic channel over distance d about frequency f is given as $A_{\text{aco}}(d, f) = A_0 d^k a(f)^d$ or

$$10 \log A_{\text{aco}}(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{13}$$

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient;[13]

$$10 \log a(f) = \frac{0.11 \cdot f^2}{1 + f^2} + \frac{44 \cdot f^2}{4100 + f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{14}$$

Attenuation in the Marine Acoustic Channel

The attenuation that occurs in an underwater acoustic channel over distance d about frequency f is given as $A_{aco}(d, f) = A_0 d^k a(f)^d$ or

$$10 \log A_{aco}(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{13}$$

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient;[13]

$$10 \log a(f) = \frac{0.11 \cdot f^2}{1 + f^2} + \frac{44 \cdot f^2}{4100 + f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{14}$$

Compared to RF Free space PL: $(A_{RF}(d, f) \approx \left(\frac{4\pi df}{c}\right)^2)$

- Exponential in d: $A_{aco} \propto f^d$ vs $A_{RF} \propto (df)^2$
- f factor four orders higher in $f \propto A_{aco}$ vs $f \propto A_{RF}$

Multi-Metric TMF - Grey Grading

$$\theta_{k,j}^t = \frac{\min_k |a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|}{|a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|} \tag{15}$$

$$\phi_{k,j}^t = \frac{\min_k |a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|}{|a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|} \tag{16}$$

$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t\right] \tag{17}$$

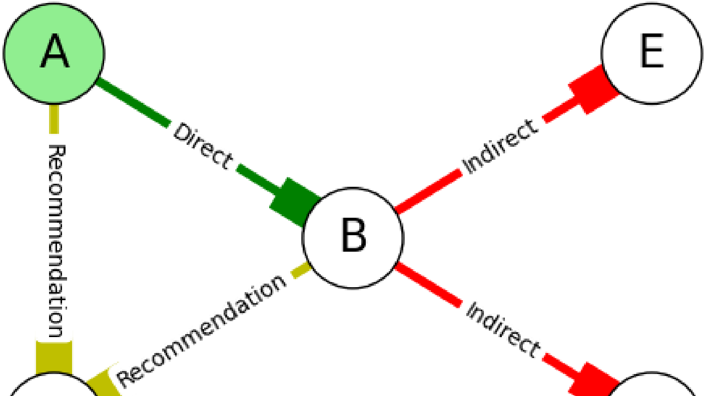
$$T_k^t = (1 + (\phi_k^t)^2/(\theta_k^t)^2)^{-1} \tag{18}$$

Where $a_{k,j}^t$ is the value of an observed metric x_j for a given node k at time t, g and b are respectively the "good" and "bad" reference metric sequences from $\{a_{k,j}^t k = 1, 2 \ldots K\}$, $H = [h_0 \ldots h_M]$ is a metric weighting vector such that $\sum h_j = 1$

Multi-Metric TMF - Topological Relationships

Includes shared assessments from other nodes weighted based on their relative topology to provide a final value[1]

$$T_{i,j}^{MTFM}$$



Grey Trust Equs I

$$
\begin{aligned}
T_{i,j}^{MTFM} = & \frac{1}{2} \cdot \max_{s}\{f_s(T_{i,j})\} T_{i,j} \\
& + \frac{1}{2} \frac{2|N_R|}{2|N_R| + |N_I|} \sum_{n \in N_R} \max_{s}\{f_s(T_{i,n})\} T_{i,n} \\
& + \frac{1}{2} \frac{|N_I|}{2|N_R| + |N_I|} \sum_{n \in N_I} \max_{s}\{f_s(T_{i,n})\} T_{i,n}
\end{aligned} \tag{19}
$$

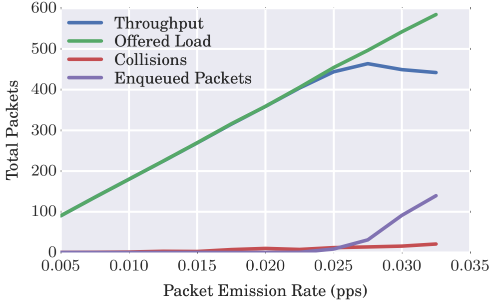
Where $T_{i,n}$ is the subjective trust assessment of n_i by n_n, and $f_s = [f_1, f_2, f_3]$ given as...

Grey Trust Equs II

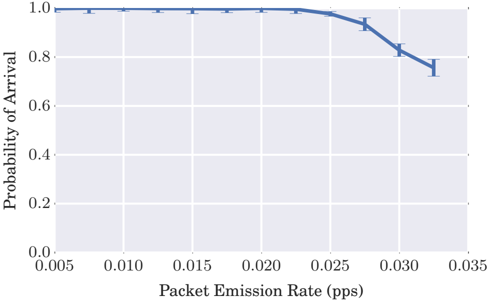
$$
\begin{aligned}
f_1(x) &= -x + 1 \\
f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\
f_3(x) &= x
\end{aligned}
\tag{20}
$$

▸ Back

Comms Scaling Graphs I

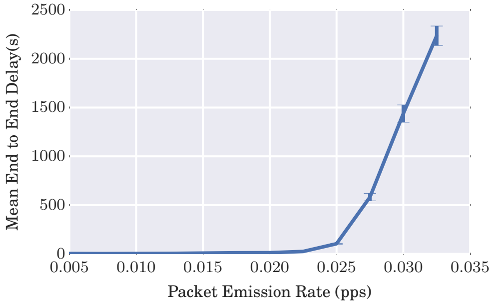


(a) Packet Delivery

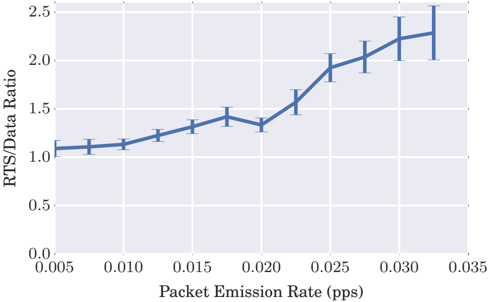


(b) Probability of arrival

Comms Scaling Graphs II



(c) End to End Delay



(d) RTS Ratios

Back

System Model Constraints

Table 3: Comparison of system model constraints as applied between Terrestrial and Marine communications ▸ Back

Parameter	Unit	Terrestrial	Marine
Simulated Duration	s	300	18000
Trust Sampling Period	s	1	600
Simulated Area	km^2	0.7	0.7-4
Transmission Range	km	0.25	1.5
Physical Layer		RF(802.11)	Acoustic
Propagation Speed	m/s	3×10^8	1490
Center Frequency	Hz	2.6×10^9	2×10^4
Bandwidth	Hz	22×10^6	1×10^4
MAC Type		CSMA/DCF	CSMA/CA
Routing Protocol		DSDV	FBR
Max Speed	ms^{-1}	5	1.5
Max Data Rate	bps	5×10^6	≈ 240
Packet Size	bits	4096	9600
Single Transmission Duration	s	10	32
Single Transmission Size	bits	10^7	9600

Metric Selection/Weighting

Table 4: ΔT_{ix} behaviour detection performance across meta-domains, including selected metrics

Domain		Behaviour ΔT_{ix} MPC	STS	Shadow	SlowCoach	Mean	Metrics in Domain $Delay$	P_{RX}	P_{TX}	S	G	PLR	$INDD$	$INHD$	$Speed$
Basic	Full	0.81	-0.03	0.42	0.60	0.45	✓	✓	✓	✓	✓	✓	✓	✓	✓
Basic	Comms	0.85	0.04	0.19	0.26	0.34	✓	✓	✓	✓	✓	✓			
Basic	Phys	0.04	0.00	0.39	0.69	0.28							✓	✓	✓
Alternate	Comms alt.	0.85	0.03	0.38	0.45	0.43				✓	✓	✓	✓		
Alternate	Phys alt.	0.48	0.03	0.42	0.63	0.39	✓	✓					✓	✓	✓