DRAFT: Trust Framework Operation in Autonomous Marine Communications Environments

In Preparation for Submission Ad-Hoc Now 2015, Athens, June 29 - July 02 2015. Deadline 20th Feb 2015

Andrew Bolster* , Alan Marshall, Ji Guo

Advanced Networks Research Group,
Department of Electrical Engineering & Electronics,
University of Liverpool, UK
{andrew.bolster,alan.marshall}@liv.ac.uk
http://www.anrg.liv.ac.uk/

Abstract. This paper presents a Trust Management Framework (TMF) for Marine Autonomous Networks, We present a comparative study on the operation and performance of such trust frameworks between a typical terrestrial and the harsh underwater communications environment, examining the scaling factors involved (periodicity, physical spacing, etc.) in comparing and contrasting these environments.
We demonstrate the need for a different approach towards metric selection and trust-timing in such constrained networks.

Keywords: ad-hoc, MANET, trust, marine, underwater, acoustic

1 Introduction

As mobile ad-hoc networks (MANETs) grow beyond the terrestrial arena, their operation and the protocols designed around them must be reviewed to assess their suitability and optimality in different communications environments to ensure their continued security, reliability, and performance.

Trust Management Frameworks (TMFs) provide information to assist the estimation of future states and operations of nodes within networks. This information is used to optimize the performance of a system of systems in the face of malicious, selfish, or defective behavior by one or more nodes within such a system. Previous research has established the advantages of implementing distributed TMFs in terrestrial, 802.11 based mobile ad-hoc networks (MANETs), particularly in terms of preventing selfish operation in constrained collaborative

* Please note that the LNCS Editorial assumes that all authors have used the western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

systems [Li and Singhal, 2007], and maintaining throughput in the presence of malicious actors [Buchegger and Le Boudec, 2002]

Current TMFs generally use a single type of observed action to derive trust metrics, i.e. successfully forwarded packets. These historical observations then inform future decisions of individual nodes, for example, the selection of a forward router with the lowest previous Packet Loss Rate (PLR) [Li et al., 2007].

Recent work has demonstrated use of a number of metrics to form a 'vector of trust. In the case of Multi-parameter trust framework for MANETs (MTFM)[Guo, 2012], these metrics related to inter-node communications. This vectorized trust allows a system to detect anomalous behavior and identify the tactics being used to undermine or subvert trust.

To date this work has been limited to terrestrial, RF based, communications networks. As autonomous underwater vehicles (AUVs) become more capable, and economical, they are being used in many defence, commercial and environmental applications. These applications are tending towards utilising independent collective behaviour of teams or fleets of these platforms [Caiti, 2011] With this use being increasingly independent of classical command and control structures, the accurate and timely establishment of mutual and distributed communications trust between nodes within such fleets is essential for the reliability and stability of such systems, and to the secure integration of such systems into larger management systems-of-systems. As such, the application of Trust methods developed in the terrestrial MANET space must be re-appraised for application within the challenging underwater communications channel.

The paper is laid out as follows. In section 2 we discuss Trust and Trust Management Frameworks, defining our terminology and reviewing the justifications for the use and development of Trust Management Frameworks. In section 3, we review selected features of the underwater communications channel, highlighting particular challenges and differentials against terrestrial equivalents. In section 4, we review the results presented in [Guo et al., 2011], including a critique of the use of Fuzzy Sets and Gray Theory and a discussion on differences in experimental configuration when transitioning from terrestrial radio to the marine space. We establish the initial parameters for simulation and set out a series of experiments to establish commonality between trust establishment in terrestrial and marine networks, characterising the communications and physical configuration with respect to the application and channel characteristics. In section **??**, we present our findings in trust establishment in this optimal network, pointing out the differences in metric selection and their impact on trust assessment stability.

Needs to be converted to prose

The contributions to the field of this paper are:

- A Trust Management Framework applicable to Underwater MANETs and why Grey Theory Analysis is particularly suited to this application.
- A study on the comparative operation and performance between terrestrial and underwater MANETs.

– A review of metric suitability for Trust Management Frameworks in marine environments, informing future metric selection for experimenters and theorists.

2 Trust and Trust Management Frameworks

2.1 Trust in MANETs

In human trust relationships it is recognised that there can be several perspectives of Trust for example organizational, sociological, interpersonal, psychological and neurological [Lee and See, 2004]. For the purposes of this work we define two perspectives on trust for autonomous systems: Design and Operational. These are summarised as follows:

– *Design Trust*; When an autonomous system is under development a level of Trust is established in it through the manner in which it has been designed and tested. This is the same as conventional systems. The difference with systems that have high-levels of autonomy is that they are designed to behave adaptively to dynamic environments that are difficult to fully predict prior to operational deployment. For example, in a navigation system it is difficult to predict the dynamic environment it will need to adapt to. So Trust needs to be developed that the design and test of such systems are sufficient to predict that operation will be, if not optimal, at least satisfactory.
– *Operational Trust*; Trust at runtime or in-situ that both the individual nodes within a system are operating as expected[1]; and that the interfaces between the operator and the system are as expected. This latter aspect covers issues such as physical/wireless links and interpretation of data at each end of such a communication link.

In addition to the two perspectives of trust identified, it is necessary to define and classify Operational Trust into two distinct but related sections, which we define as being:

– *Hard Trust* or technical trust, being the quantitative measurement and communication of the expectation of an actor performing a certain task, based on historic performance and through consensus building within a networked system. Can be thought of as a de-risking strategy to measure and monitor the ability of a system, or another actor within a system, to perform a task unsupervised.
– *Soft Trust* or common trust, being the qualitative assessment of the ability of an actor to perform a task or operation consistently and reliably based on social or experiential factors. This is the natural form of trust and is the main motivational driver for the human-factors trust discussion. Can be rephrased as the level of confidence an operator has in an actor to perform a task unsupervised.

[1] Operational Trust is functionally derived from, but distinct from Design Trust

For the purposes of this work, we are concerned with the analytical establishment of hard trust within a topologically dynamic network of autonomous actors.

2.2 Current Trust Management Frameworks

Various models and algorithms for describing trust and developing trust management in distributed systems, P2P communities or wireless networks have been considered. Taking some examples;

- *The Objective Trust Management Framework* takes a Bayesian approach and introduces the idea of applying a Beta function to changes in the per-link Packet Loss Rate (PLR) over time as an encapsulation method, combining "Trust" and "Confidence of Assessment" into a single value [Li et al., 2007]. OTMF however does not appropriately combat multi-node-collusion in the network [Cho et al., 2011].
- *Trust-based Secure Routing [Moe et al., 2008]* demonstrated an extension to Dynamic Source Routing (DSR), incorporating a Hidden Markov Model of the wider ad-hoc network, reducing the efficacy of Byzantine attacks, particularly black-hole attacks but, along with many more TMFs surveyed in [Cho et al., 2011], falls under the same limitation of focusing on single metric observation (PLR).
- *CONFIDANCE*; [Buchegger and Le Boudec, 2002] presented an approach using a probabilistic estimation of normal observations, generating a posterior probability distribution of node forwarding behaviours, similar to OTMF. They also introduced a a greedy topology weighting scheme that internally weighted incoming trust assessments based on historical experience of the reporter.

These single metric TMFs provide malicious actors with a significant advantage if their activity is undetectable by that one assessed metric, especially if the attacker knows the metric in advance.

The objective of operating a TMF is to increase the confidence in, and efficiency of, a system by reducing the amount of undetectable negative operations an attacker can perform. This "set" of potential attacks can be described as a "threat surface". In the case where the attacker can subvert the TMF, the metric under assessment by that TMF does not cover the threat mounted by the attacker. In turn, this causes a super-linearly negative effect in the efficiency of the network as the TMF is assumed to have reduced the threat surface when in fact it has only made it more advantageous to attack a different aspect of the networks operation. An example of such a behaviour would be the case in a TMF focused on PLR where an attacker selectively delays packets going through it, reducing the over all throughput of one or more virtual network routes. Such behaviour would not be detected by the TMF. [Huang et al., 2010] also raised the need for a more expanded view of trust but did so with a domain-partitioning approach rather than combining trust assessments from multiple domains within networks.

doesn't follow from rest of paragraph, needs to be expanded to explain the domain approach, possibly move back to 'future work' or something

Need to lead from single metric assessment to multi-metric

2.3 Grey Relational Trust for Terrestrial MANETs

[Guo, 2012] demonstrated the ability of Grey Relational Analysis (GRA)[Zuo, 1995] to normalize and operationally combine disparate traits of a communications link such as instantaneous throughput, received signal strength, etc. into a single comparable value, a Grey Relational Coefficient, or a "trust vector".

In the case of the terrestrial communications network used in [Guo, 2012], the observed metric set $X = \{x_1, \ldots, x_M\}$ representing the measurements taken by each node of its neighbours at least interval, is defined as

$$X = \{\text{packet loss rate, signal strength, data rate, delay, throughput}\} \tag{1}$$

The trust vector is then given as

$$\theta^t_{k,j} = \frac{\min_k |a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|}{|a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|} \tag{2}$$

$$\phi^t_{k,j} = \frac{\min_k |a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|}{|a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|} \tag{3}$$

$$[\theta^t_k, \phi^t_k] = [(\theta^t_{k,0}, \ldots, \theta^t_{k,M}), (\phi^t_{k,0}, \ldots, \phi^t_{k,M})] \tag{4}$$

where $a^t_{k,j}$ is the value of a observed metric x_j for a given node k at time t, ρ is a distinguishing coefficient normally set to 0.5, g and b are respectively the 'good' and 'bad' reference metric sequences from $\{a^t_{k,j}, k = 1, 2 \ldots K\}$, e.g. $g_j = \max_k(a^t_{k,j})$, $b_j = \min_k(a^t_{k,j})$ (where each metric is selected to be monotonically increasingly positive for trust assessment, e.g. throughput). θ and ϕ are then scaled to $[0, 1]$ using the mapping $y = 1.5x - 0.5$. The vector natures of $[\theta^t_k, \phi^t_k]$ allow per-metric weighting before generating a single trust assessment, and also allows the identification and classification of untrustworthy agents. These weighted $[\theta, \phi]$ values are then condensed into a single trust value by

$$T^t_k = \frac{1}{1 + \frac{(\phi^t_k)^2}{(\theta^t_k)^2}} \tag{5}$$

There are situations where the observed metrics will include significant noise involved with complicated interdependencies between the environment and the system under observation; and those observations themselves occur at irregular, sparse, intervals. In such cases, conventional approaches such as Bayesian prior probability estimation do not produce trust values that fairly reflect the underlying metrics, as they require a-prioi assumption that the trust value under exploration has a known or expected distribution (Beta), that that distribution is monomodal, and that the input metrics are binary discernible. These assumptions are required to scale and classify resultant trust values to a stable assessment range (usually $[0, 1]$) [Liu, 2006]. In scenarios with variable, sparse, noisy

metrics, estimating the distribution is difficult to accomplish off-line in advance. Further, the binary requirement of Bayesian-style modelling requires internal discriminating logic, which discards useful information from a multi-node perspective, and generating a phase transition area where a proportion of negative or malicious behaviour does not impact the assessed trust observations of other nodes, but still impacts system performance [Mundinger and Boudec, 2008]

could be worded differently

Grey Theory counters this by performing cohort based normalisation of arbitraty-dimensional metrics at runtime. This creates a more stable contextual assessment of trust, providing an "extent" of potential trust values with respect to other observed nodes in that interval rather, while still maintaining the ability to reduce trust values down to a stable assessment range for decision support without having to characterise every environment entered into.[2]

GRA, combined with a fuzzy whiteization model (6), and a topology-aware weighting scheme(7) [3] provide capability to both detect the existence of a malicious agent within the network, and to classify what trust metrics that attacker is manipulating.

There are three classes of topological trust relationship; Direct, Recommendation, and Indirect. To take the example of a node n_i monitoring the trust of another, target, node, n_j; the Direct relationship is simply the trust assessment based on n_i's own observations and experience of n_j's behaviour. In the Recommendation case, another node, n_k, which shares direct relationships with both n_i and n_j, gives it's opinion on the trustworthiness of n_j to n_i. The Indirect case is similar to the recommendation case, except that the recommender n_k, does not have a (current) direct link with the target n_j but that has a direct link with the observer node, n_i.

These relationships give us node sets, N_R and N_I containing the nodes that have recommendation or indirect, relationships to the observing node respectively.

$$
\begin{aligned}
f_1(x) &= -x + 1 \\
f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\
f_3(x) &= x
\end{aligned}
\tag{6}
$$

[2] A potential negative to this approach is that since the assessment is relative in nature (as opposed to the absolutist approach to trust assumed in other frameworks), even in ideal operating networks, nodes will receive middling trust assessments, as there is no-one else "bad" to compete against. Future work will investigate the stability of GRA under multi-node collusion

[3] similar to that employed in CONFIDANT

$$
\begin{aligned}
T_{i,j}^{net} = & \frac{1}{2} \cdot \max_s \{f_s(T_{i,j})\} T_{i,j} && \text{Direct Trust} \\
& + \frac{|N_R|}{2|N_R| + |N_I|} \sum_{n \in N_R} \max_s \{f_s(T_{i,n})\} T_{i,n} && \text{Recommendation Trust} \\
& + \frac{|N_I|}{2|N_R| + |N_I|} \sum_{n \in N_I} \max_s \{f_s(T_{i,n})\} T_{i,n} && \text{Indirect Trust}
\end{aligned} \tag{7}
$$

2.4 Scenarios

Maybe move to Section 4

Four Mobility scenarios were used in [Guo et al., 2011] to explore the trust-behaviour, covering the majority of MANET operational requirements;

- All Nodes Static
- Central node performing a random walk with leaf-nodes static
- Leaf-nodes randomly walking with central node static
- All nodes randomly walking

The six nodes are arranged as per Fig. 1, such that each node is on average 100m from its neighbours. The use of six nodes and the particular layout enables the investigation of the three trust relationships based on minimum path topologies, such that the node generating the trust assessments, n_0 has Direct, Recommendation, and Indirect trust assessments available to it from itself, $[n_2, n_3]$, and $[n_4, n_5]$ respectively.

In all of the scenarios, each link from $n_i \rightarrow n_j$ sent 10 second bursts of Constant Bit Rate (CBR) style traffic.

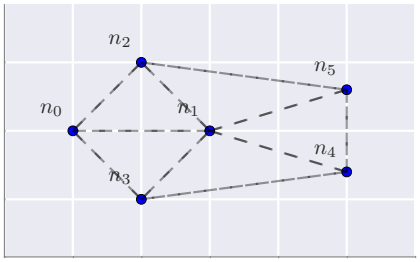


Fig. 1: Initial Scenario Topology, with nodes spaced an average of 100m apart

Guo demonstrated that when compared against OTMF and Beta trust assessment, MTFM provided increased variation in trust assessment over time, providing more information about the nodes behaviour than simply the probabilistic nature of packet delivery. Guo also demonstrated that this MTFM valuation was stochastically stable for varying mobilities.

3 Marine Acoustic Networks

The key challenges of underwater acoustic communications are centred around the impact of slow and differential propagation of energy (RF, Optical, Acoustic) through water, and it's interfaces with the seabed / air. The resultant challenges include; long delays due to propagation, significant inter-symbol interference and Doppler spreading, fast and slow fading due to environmental effects (aquatic flora/fauna; surface weather), carrier-frequency dependent signal attenuation, multipath caused by the medium interfaces at the surface and seabed, variations in propagation speed due to depth dependant effects (salinity, temperature, pressure, gaseous concentrations and bubbling), and subsequent refractive spreading and lensing due to that same propagation variation[Partan et al., 2006].

The attenuation that occurs in an underwater acoustic channel over a distance d for a signal about frequency f in linear and dB forms respectively is given by

$$A(d, f) = A_0 d^k a(f)^d \tag{8}$$

$$10 \log A(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{9}$$

where A_0 is a unit-normalising constant, k is a spreading factor (commonly taken as 1.5), and $a(f)$ is the absorption coefficient, expressed empirically using Thorp's formula (10) from [Stojanovic, 2007]

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

Thus, the multi-path channel transfer function can be described by

$$H(d, f) = \sum_{p=0}^{P-1} h(p) = \sum_{p=0}^{P-1} \Gamma_p / \sqrt{A(d_p, f)} e^{-j2\pi f \tau_p} \tag{11}$$

where $d = d_0$ is the minimal path length between the transmitter and receiver, $d_p, p = \{1, \ldots P-1\}$ are the secondary path lengths, Γ_p models additional losses incurred on each path such as reflection losses at the surface interface, and $\tau_p = d_p/c$ is the delay time ($c = 1500ms^{-1}$ is the nominal speed of sound underwater).

This combination of refractive lensing and the multipath nature of the medium result in supposedly "line of sight" propagation being extremely unreliable for estimating distances to targets, as the first arriving beam has as the very least bent in the medium, and commonly has bounced between the surface/seabed before arriving at a receiver. Further, this affect is usually anisotropic with differential depths between transmitter and receiver, meaning that any variation in depth across a channel, greatly impacts the characteristics of that channel.

Comparing (8) with the RF Free-Space Path Loss model (12), while both are frequency and distance dependant;

$$A_{rf}(d,f) \approx \left(\frac{4\pi f}{c}\right)^2 \text{ where } c \approx 3 \times 10^8 m/s \tag{12}$$

3.1 Trust in Marine Networks

In this subsection we establish the requirement for communications trust in acoustic marine networks, extending and expanding on the generic assessment given in 2.1

Justify Why Grey, discuss current uses and demand. Relate back to Section 2.1

4 Initial System Model Characterisation

4.1 Simulation Background

Simulations were conducted using a Python based agent simulation framework based on SimPy[Müller and Vignaux, 2003], with a network stack built upon the AUVNetSim stack[Miquel and Montana, 2008], with transmission parameters (Table 1) taken from and validated against [Stojanovic, 2007] and [Stefanov and Stojanovic, 2011].

Given the differences in delay and propagation between RF and marine networks, it is natural that the same application rates (e.g. packet emission rates or throughput) cannot be maintained under such different constraints. Therefore, before we can fairly assess the trust operation of a Underwater MANET, we first establish it's operational characteristics.

We define a methodology for establishing an comparative operating point in the marine environment that can account for the differences in communications environment while maintaining a comparable trust operation. This was done in two parts; optimisation for Communications Rate, optimisation for Physical Distribution.

4.2 Establishing Scale Factors in Communications Rate

In this section we characterise the simulated communications environment, establishing an optimal packet emission rate for comparison against [Guo et al., 2011].

In order to establish the point at which the network becomes saturated due, a range of packet emission rates were explored between 0.01 packets per second (pps), equivalent to 96 bps, up to 0.07 pps (672 bps)

From Figs. 2 and 3, it is clear that the threshold curve, expressed as the *Successfully Received Packets* line, exhibits a saturation point between 0.025 and 0.03 pps. Particularly in Fig. 3, the precipitous drop in packet delivery probability beyond 0.025 pps, indicating that this is a strong candidate value for an upper-limit to the safe operating zone in terms of packet emission.

Table 1: Comparison of system model constraints as applied between Terrestrial and Marine communications

Parameter	Unit	Terrestrial	Marine
Simulated Duration	s	300	36000
Simulated Area	km^2	0.7	Various
Transmission Range	km	0.25	1.5
Number of Nodes		6	6
Physical Layer		RF(802.11)	Acoustic
Propagation Speed	m/s	3×10^8	1490
Center Frequency	Hz	2.6×10^9	10^3
Bandwidth	Hz	22×10^6	10^3
MAC Type		CSMA/CA	CSMA/CA
Routing Protocol		DSDV	FBR
Mobility		Various	Various
Max Speed	ms^{-1}	5	1.25
Data Rate	bps	10^6	240
Burst Counts		10	1
Packet Size	bits	4096	9600
Destination Selection		Random	Random
Single Transmission Duration	s	10	32
Single Transmission Size	bits	10^7	9600

possibly need to further justify large packets explicitly rather than just pointing at milicia

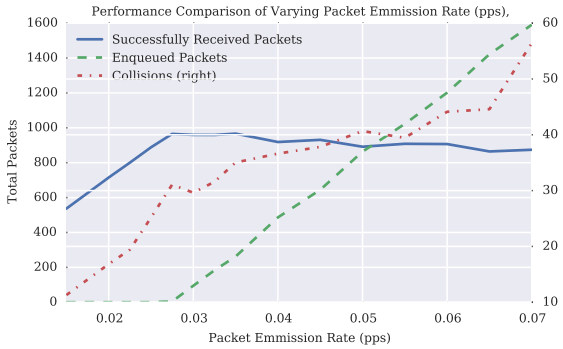


Fig. 2: Varying packet emission rate demonstrates maximal throughput at 0.025 packets per second, equivalent to ≈240 bps

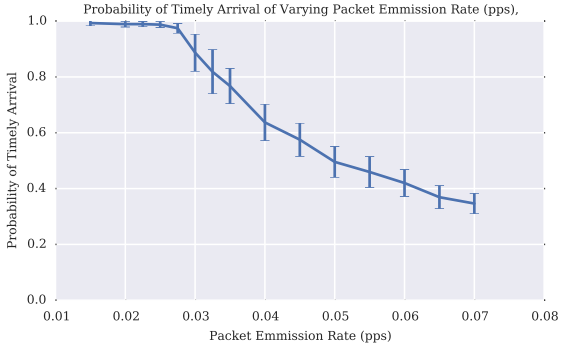


Fig. 3: Varying packet emission rate demonstrates a saturation point at 0.025 packets per second

4.3 Establishing Scale Factors in Physical Distribution

In this section we characterise the effect of node-separation scaling on communications operation for comparison against [Guo et al., 2011]. This is particularly important considering the significant scale factor differences between not only the speed of propagation in the medium, but simply the range of operation. From Table 1, the operating transmission range of acoustic is ≈ 6 times further than 802.11. Therefore, a reasonable experimental range would have an upper bound of performance around this scaling factor, where nodes are approximately $600m$ apart.

A reasonable range around this is to scale from $100m$ apart on average to $1000m$.

Varying average node separation shows that while direct throughput isn't significantly affected until, collision rates are Fig. 4. This collision rate is well within the tolerances of the MAC layer, as shown in Fig. 5, where even with a rising collision rate, packets are being reliably received.

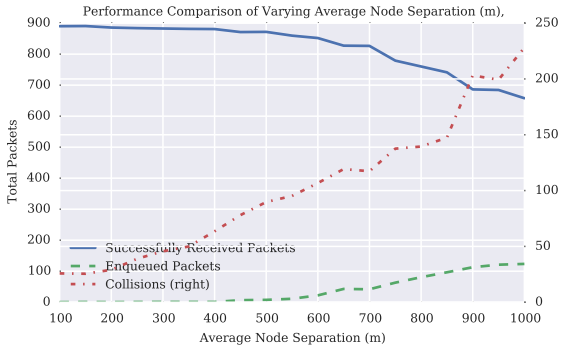


Fig. 4: Comparison of Medium Acquisition Collisions, Throughput, and Enqueued packets against varying application packet emission rates.

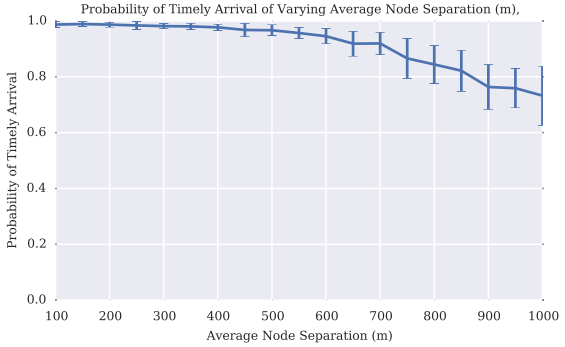


Fig. 5: Probability of Timely Reception across a range of node scaling.

However, when end-to-end delay is investigated, it's clear from Fig. 6 that the network is becoming severely impaired approaching the $700m$ mark, with delays rising to more than 25 minutes above $700m$. This is also demonstrated by the increasing RTS/Data ratio shown in Fig. 7. At According to Xu [Xu et al., 2002], the RTS/CTS handshake cannot function well as interference protection at node separations beyond 0.56 times the transmission range. This is also demonstrated in Fig. 7, where above $1500m \times 0.56 = 840m$, This is due to reduced channel availability due to collisions, which are then due to a much longer potential contention period between nodes.

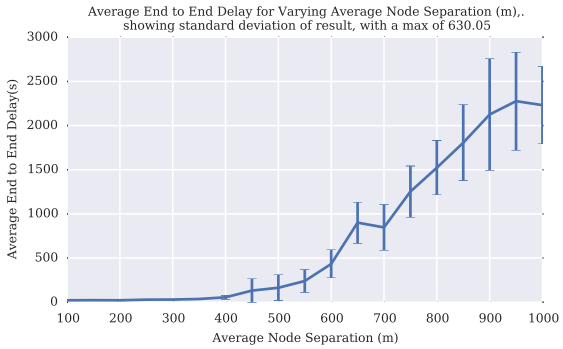


Fig. 6: End to End Delay under varying node-separations

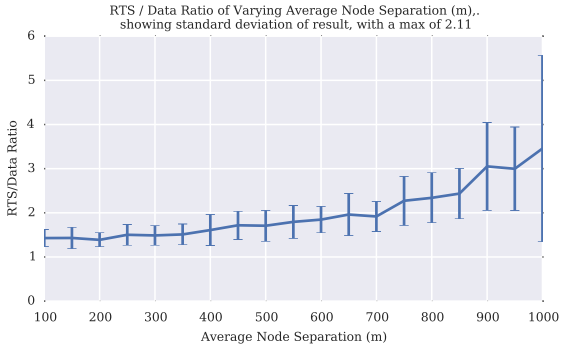


Fig. 7: RTS/Data ratio for farying node-separations

Table 2: Tabular view of data from Figs 5, 6, and 7

Separation(m)	Delay(s)	Probability of Arrival	RTS/Data Ratio	Ideal Delivery Time(s)
100	21.88	0.99	1.43	1.03
150	23.23	0.99	1.43	1.07
200	21.78	0.99	1.39	1.10
250	28.94	0.98	1.50	1.14
300	30.31	0.98	1.49	1.17
350	36.41	0.98	1.51	1.21
400	55.63	0.98	1.61	1.25
450	131.67	0.97	1.72	1.28
500	163.58	0.97	1.71	1.32
550	240.06	0.96	1.80	1.35
600	433.12	0.95	1.85	1.39
650	901.09	0.92	1.96	1.42
700	847.05	0.92	1.92	1.46
750	1253.23	0.87	2.27	1.50
800	1522.80	0.84	2.34	1.53
850	1805.63	0.82	2.44	1.57
900	2125.33	0.76	3.05	1.60
950	2276.76	0.76	3.00	1.64
1000	2231.69	0.73	3.46	1.67

4.4 Scaling Discussion

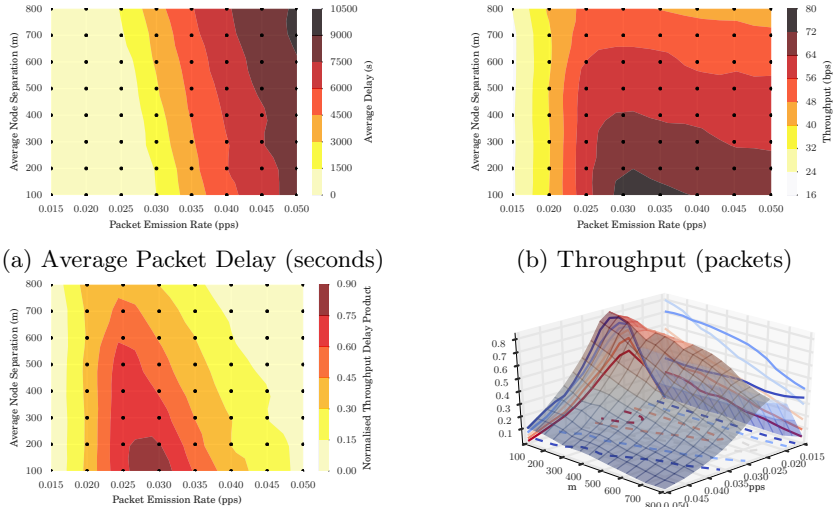
We establish a appropriate safe operating zone for marine communications by looking at the communications rate and physical distribution factors together as a 3D surface. We select throughput and end to end delay as the targeted aspects of the networks performance to optimise against. The raw results of these two facets are shown in Fig. 8.

Normalising each of these results to the range $[0, 1]$ by $X' = \frac{X - \min(X)}{\max(X) - \min(x)}$, and taking the product of these normalised values gives a qualitative illustration of the 'goodness' of the performance surface, shown in Fig. 8c. These results indicate that the best area to continue operating in for a variety of node separations is at 0.025pps, and that a reasonable position scaling is from 100m to 600m, beyond which communication becomes increasingly unstable.

5 Trust

1.

All the 'programming' for this bit is done, it's just writing. Remember to highlight the relationships between delay/distance/trust and rssi/plr/trust



(a) Average Packet Delay (seconds)

(b) Throughput (packets)

(c) Normalised Product

(d) Normalised Surface Plot

Fig. 8: Field of Results for Varying Packet Emission Rates and Node Separations.

Acknowledgments. The heading should be treated as a subsubsection heading and should not be assigned a number.

6 The References Section

References

Buchegger and Le Boudec, 2002. Buchegger, S. and Le Boudec, J.-Y. (2002). Performance analysis of the CONFIDANT protocol. *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc '02*, pages 226–236.

Caiti, 2011. Caiti, A. (2011). Cooperative distributed behaviours of an AUV network for asset protection with communication constraints. *OCEANS, 2011 IEEE-Spain*.

Cho et al., 2011. Cho, J.-h., Swami, A., and Chen, I.-r. (2011). A survey on trust management for mobile ad hoc networks. *Communications Surveys & Tutorials*, 13(4):562–583.

Guo, 2012. Guo, J. (2012). Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks.

Guo et al., 2011. Guo, J., Marshall, A., and Zhou, B. (2011). A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks. *2011IEEE 10th International Conference on Trust Security and Privacy in Computing and Communications*, pages 142–149.

Huang et al., 2010. Huang, D., Hong, X., and Gerla, M. (2010). Situation-aware trust architecture for vehicular networks. *Communications Magazine, IEEE*, (November):128–135.

Lee and See, 2004. Lee, J. D. and See, K. A. (2004). Trust in automation: designing for appropriate reliance. *Human factors*, 46(1):50–80.

Li and Singhal, 2007. Li, H. and Singhal, M. (2007). Trust Management in Distributed Systems. *Computer*, 40(2):45–53.

Li et al., 2007. Li, J., Li, R., Kato, J., Li, J., Liu, P., and Chen, H.-H. (2007). Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Communications Magazine*, 46(4):108–114.

Liu, 2006. Liu, K. J. R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*, 24(2):305–317.

Miquel and Montana, 2008. Miquel, J. and Montana, J. (2008). AUVNetSim: A Simulator for Underwater Acoustic Networks. *Program*, pages 1–13.

Moe et al., 2008. Moe, M. E. G., Helvik, B. E., and Knapskog, S. J. (2008). TSR: Trust-based secure MANET routing using HMMs. *... Symp. QoS Secur. ...*, pages 83–90.

Müller and Vignaux, 2003. Müller, K. and Vignaux, T. (2003). SimPy: Simulating Systems in Python. *ONLamp.com Python DevCenter*.

Mundinger and Boudec, 2008. Mundinger, J. and Boudec, J. L. (2008). Analysis of a reputation system for mobile ad-hoc networks with liars. *Performance Evaluation*, pages 0–5.

Partan et al., 2006. Partan, J., Kurose, J., and Levine, B. N. (2006). A survey of practical issues in underwater networks. *Proceedings of the 1st ACM international workshop on Underwater networks WUWNet 06*, 11(4):17.

Stefanov and Stojanovic, 2011. Stefanov, A. and Stojanovic, M. (2011). Design and performance analysis of underwater acoustic networks. *IEEE Journal on Selected Areas in Communications*, 29(10):2012–2021.

Stojanovic, 2007. Stojanovic, M. (2007). On the relationship between capacity and distance in an underwater acoustic communication channel.

Xu et al., 2002. Xu, K., Gerla, M., Bae, S., and Networks, H. (2002). Effectiveness of RTS / CTS Handshake in IEEE. *..., 2002. Globecom'02. Ieee*, 56:1–14.

Zuo, 1995. Zuo, F. (1995). Determining Method for Grey Relational Distinguished Coefficient. *SIGICE Bull.*, 20(3):22–28.

Todo list