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 behaviour 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 systems [7], and maintaining throughput in the presence of malicious actors [1]

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) [8].

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)[4], these metrics related to inter-node communications. This vectorized trust allows a system to detect anomalous behaviour 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 [2] With this use being increasingly independent of classical command and control structures, the establishment of trust between nodes is essential for the reliability and stability of such teams. 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 establish an experimental configuration for the marine space, and we review the scenarios and results presented in [5]. In Section 5, we present our findings in trust establishment and malicious behaviour detection, comparing with OTMF and Beta.

The contributions to the field of this paper are: A Trust Management Framework applicable to Underwater MANETs, a study on the comparative operation and performance between terrestrial and underwater MANETs using TMFs, and 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

Trust is the level of confidence one agent has in another to perform a given action on request or in a certain context. Trust in the autonomous or semi-autonomous realm is the ability of a system to establish and maintain confidence in itself or another systems' operations. Managing this trust can be used to predict and reason on the future interactions between entities in a system, such as an autonomous mobile ad-hoc network (MANET).

The distributed and dynamic nature of MANETs mean that it is difficult to maintain a trusted third party (TTP) or evidence based trust system such as Certificate Authorities or using Public Key Infrastructures (PKI). Therefore, a distributed, collaborative system must be applied to these networks. Such distributed trust management frameworks aim to detect, identify, and mitigate the impacts of malicious actors by distributing per-node assessments and opinions to collectively self-police behaviour.

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, combining "Trust" and "Confidence of Assessment" into a single value [8]. OTMF however does not appropriately combat multi-node-collusion in the network [3].
- *Trust-based Secure Routing [12]* 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 is limited by focusing on single metric observation (PLR)[3].
- *CONFIDANT*; [1] presented an approach using a probabilistic estimation of normal observations, similar to OTMF. They also introduced a greedy topology weighting scheme that internally weighted incoming trust assessments based on historical experience of the reporter.
- *Fuzzy Trust-Based Filtering*; [10] presented a method using Fuzzy Inference to cope with imperfect or malicious recommendation based on a probabilistic estimation of performance using conditional similarity to classify performance using overlapping Fuzzy Set Membership functions to collaboratively filter reputations across a network.

OTMF, CONFIDANT, and Fuzzy Trust-Based Filtering can be generalised as single-value probabilistic estimation, based around a Bayesian idea of taking a binary input state and generating an idealised Beta Distribution of the future states of that input. This expectation value is $\text{beta}(p|\alpha,\beta) \rightarrow E(p) = \frac{\alpha}{\alpha+\beta}$ where α and β represent the number of successful and unsuccessful interactions respectively.

These single metric TMFs provide malicious actors with a significant advantage if their activity is undetectable by that 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. 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 possible set of attacks 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.

2.3 Grey Theory Operation

There are situations where the observed metrics will include significant noise and those observations occurring 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 success or failure. These assumptions are required to scale and classify resultant trust values to a stable assessment range (usually $[0, 1]$) [9]. 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 or classification logic, which if applied to non-binary inputs, discards useful information and generates a phase transition area where a proportion of negative or malicious behaviour does not impact the assessed trust values, but still impacts system performance [14].

Finally, there is no accounting for the context in which the assessment is taking place; while OTMF does include topological information, it does not take account of environmental factors that may be inducing poor performance. Grey Theory counters this by performing cohort based normalisation of 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. This presents a stark difference between the Grey System and Probalistic approaches. In Grey, assessments are relative in nature even in fairly operating networks. Nodes will generally receive middle-range trust assessments if there are no malicious actors as there is no-one else "bad" to compete against. Future work will investigate the stability of GRA under multi-node collusion.

Add to future work section

Table 1 provides a qualitative summary of the differences in use and application between Fuzzy, Probabilistic and Grey Systems of managing uncertainty.

Guo[4] demonstrated the ability of Grey Relational Analysis (GRA)[20] 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 [4], 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

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

The trust vector is given as

Table 1: Comparison between selected methods of characterising uncertainty, adapted from [5] [9] [15] [19]

	Fuzzy Math	Bayesian Estimation	Grey Systems
Objects	Cognitive Uncertainty	Distribution Refinement	Poor Information
Set Style	Fuzzy Sets	Cantor Sets	Grey Hazy Sets
Processes	Marginal Sampling	Frequency Distribution	Sequence Generation
Requirement	Known Membership	Beta Distribution	Any Distribution
Emphasis	Extension	Intension	Intension
Characteristics	Experience	Large Samples	Small Samples

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

$$\phi_{k,j}^t = \frac{\min_k |a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|}{|a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|} \tag{3}$$

where $a_{k,j}^t$ 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 $\{a_{k,j}^t k = 1, 2 \dots K\}$, e.g. $g_j = \max_k(a_{k,j}^t)$, $b_j = \min_k(a_{k,j}^t)$ (where each metric is selected to be monotonically increasingly positive for trust assessment, e.g. throughput).

Weighting can be applied weighting before generating a single trust assessment, which we will show also allows the identification and classification of untrustworthy agents.

θ and ϕ are then scaled to $[0, 1]$ using the mapping $y = 1.5x - 0.5$.

$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t \right] \tag{4}$$

Where $H = [h_0 \dots h_M]$ is a metric weighting vector such that $\sum h_j = 1$, and in the basic case, $H = [\frac{1}{M}, \frac{1}{M} \dots \frac{1}{M}]$ to treat all metrics evenly. These weighted $[\theta, \phi]$ values are then condensed into a single trust value by

$$T_k^t = \frac{1}{1 + \frac{(\phi_k^t)^2}{(\theta_k^t)^2}} \tag{5}$$

This trust value minimises the uncertainties of belonging to either best (g) or worst (b) sequences in (2).

GRA, combined with a fuzzy whiteisation model (6), and a topology-aware weighting scheme(7) 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 observer n_i but that has a Direct link with the target node, n_j.

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.

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

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

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[16].

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

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

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

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 [18]

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

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

$$H(d, f) = \sum_{p=0}^{P-1} h(p) = \sum_{p=0}^{P-1} \Gamma_p / \sqrt{A(d_p, f)} e^{-j2\pi f \tau_p} \tag{11}$$
$$\text{where } \tau_p = d_p/c, c \approx 1500 ms^{-1}$$

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 ($c \approx 1500 ms^{-1}$ 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, creating secondary paths that are sometimes many times longer than the first arrival path, generating symbol spreading over orders of seconds depending on the ranges and depths involved. Further, this affect is usually anisotropic with different 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), the impact of range on signal power is exponential underwater, rather than quadratic in RF space ($A_{\text{aco}} \propto f^{2d}$ vs $A_{\text{RF}} \propto (df)^2$). While both frequency dependant factors are quadratic, approximating the factors in (10), $f \propto A_{\text{aco}}$ is at least 4 orders of magnitude higher than $f \propto A_{\text{RF}}$

$$A_{\text{RF}}(d, f) \approx \left(\frac{4\pi df}{c}\right)^2 \text{ where } c \approx 3 \times 10^8 ms^{-1} \tag{12}$$

3.1 Trust in Marine Networks

In this subsection we establish the requirement for communications trust in

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

acoustic marine networks, extending and expanding on the generic assessment given in 2.1. With increasing demand for smaller, more decentralised marine survey and monitoring systems, and a drive towards lower per-unit cost, TMFs are going to be increasingly applied to the marine space, as in theory, the benefits they would present are significant. Beyond the constraints of the communications environment (Section 3), the move towards smaller decentralised systems has knock on pressures in terms of battery capacity, onboard processing, locomotion, and prioritisation of sensor payloads to name but a few. These pressures simultaneously present opportunities and incentives for malicious or selfish actors to appear to cooperate fairly while not reciprocating that fairness in order for instance to conserve power. These multiple aspects of potential incentives, trust, and fairness clearly do not fall under the purview of single metric trusts such as OTMF, CONFIDANT, etc., and this context indicates that a multi-metric approach should provide more actionable results.

4 Initial System Model Characterisation

4.1 Mobility, Topology, and Communications Payloads

Four Mobility scenarios were used in [5] to explore trust behaviour, covering the majority of MANET operational requirements; all nodes static, a central node n_1 performing a random walk with other nodes remaining static, all nodes but the central node (n_1) randomly walking, and 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.

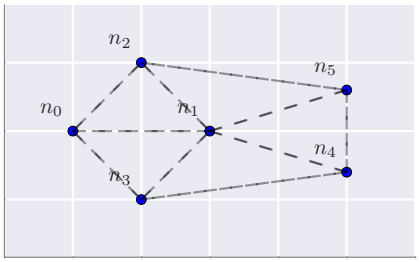


Fig. 1: Initial Scenario Topology, with nodes spaced an average of 100m apart

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. By dynamically weighting the metrics used in MTFM, it was shown that the trust assessments could be used to identify the style of misbehaviour being performed within the network and by who.

We present a corollary method to investigate and apply this work to the Marine MANET field.

4.2 Simulation Background

Simulations were conducted using a Python based agent simulation framework based on SimPy[13], with a network stack built upon the AUVNetSim stack[11], with transmission parameters (Table 2) taken from and validated against [18] and [17].

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) and node separations should not be assumed to be equivalent. Therefore, we characterise an operational zone of performance within which the network can operate normally.

Table 2: 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	2×10^4
Bandwidth	Hz	22×10^6	1×10^4
MAC Type		CSMA/DCF	CSMA/CA
Routing Protocol		DSDV	FBR
Mobility		Various	Various
Max Speed	ms^{-1}	5	2.4
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

4.3 Scaling Considerations between Terrestrial and Underwater Environments

In this section we characterise the simulated communications environment, establishing an optimal packet emission rate for comparison against [5].

We establish a appropriate safe operating zone for marine communications by looking at the communications rate and physical distribution factors together across the four presented scenarios. In scaling the physical distribution of the nodes, we also scale the environment in which the nodes are restricted to, which has a significant impact on the number of potential runtime topologies, with nodes getting increasingly isolated as the environment space increases, leading to increasing packet losses and delays as routes are constantly broken, re-advertised and re-established. From Table 2, the operating transmission range of this model of acoustic communications is ≈ 6 times further than 802.11, indicating that a suitable operating environment will have an area $\approx \sqrt{6}$ times the area of the 802.11 case. However, it was recognised in Section 3 that the relationship between attenuation and distance is exponential underwater, so this would represent an upper bound of performance, where nodes begin approximately $400m$ apart.

We select throughput and end to end delay as the targeted aspects of the networks performance to optimise against. We take the ratio of throughput per second of delay as a combined proxy for this optimisation. T/d, shown in Fig. 3.

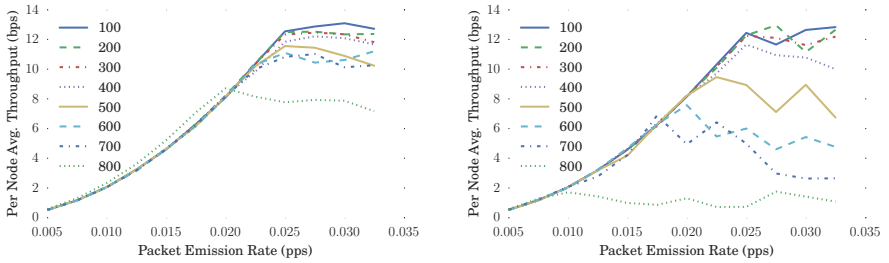
As the separation is increased, the emission rate at which the network becomes saturated decreases, reducing overall throughput. This throughput degradation is tightly coupled with the mobility scenario. For instance, in Fig. 2a, where all nodes are static, we do not see significant drops in saturation rates until we approach 800m, nearly double our estimate. However, in Figs. 2c and 2d, where the majority or all the nodes are randomly walking, and the saturation point collapses from 0.025pps at 300m to 0.015pps at 400m.These results indicate that the best area to continue operating in for a variety of node separations is at 0.015pps, and that a reasonable position scaling is from 100m to 300m, beyond which communication becomes increasingly unstable, especially in terms of end to end delay.

Add in Table here for delay characteristics too and talk about that, drawing the conclusion that 300 is better than 400 because you can increase the emission rate!

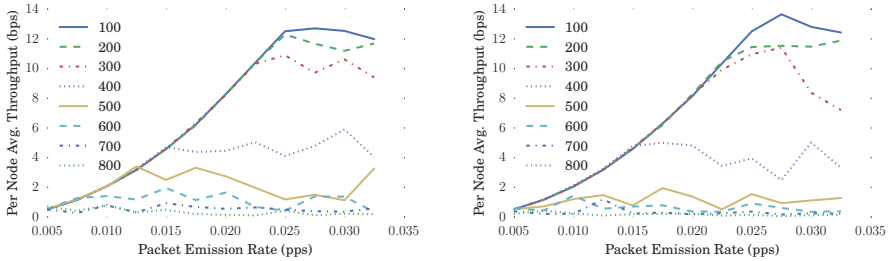
5 Trust

Having established a safe operating range for comparison, at 300m separation with an emission rate of 0.015pps, we proceed to repeat the scenarios presented in [5]. We select an assessment period of 10 mins within a 5 hour 'mission' to scale in comparison to the relative bitrates experienced (1Mbps vs $approx$15bps).

The metrics available in this marine network do not universally match their counterparts in the 802.11 network in [5] Initially, all the available metrics (transmitted and received throughput, delay, received signal strength, transmitted power, and packet loss rate as calculated by aborted, unacknowledged, transmissions) were utilised for Grey assessment. Compared to [5], this metric set lacks a data rate quantity as the network is not dynamically adjusting bandwidth. In

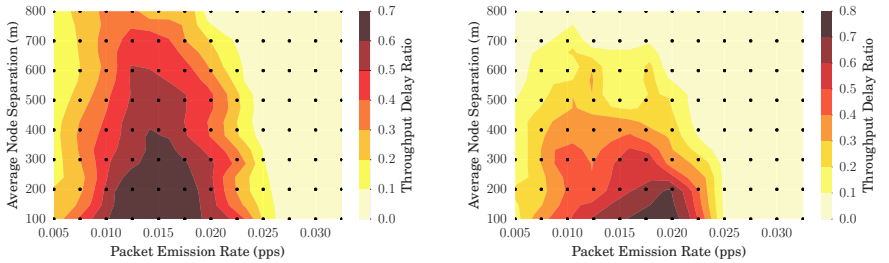


(a) All Nodes Static (b) n_1 Random Walk

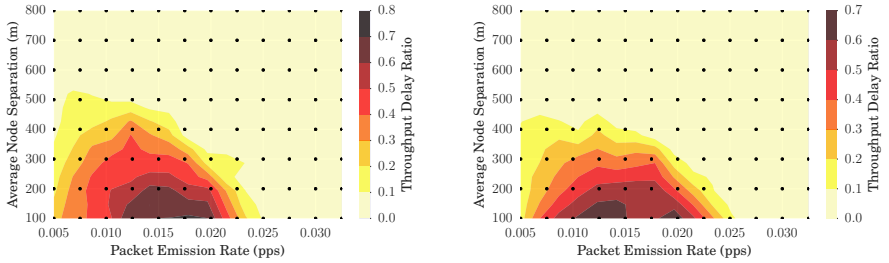


(c) All nodes but n_1 Random Walk (d) All Nodes Mobile

Fig. 2: Throughput Characteristics for varying node separations across increasing packet emission rates



(a) All Nodes Static (b) n_1 Random Walk



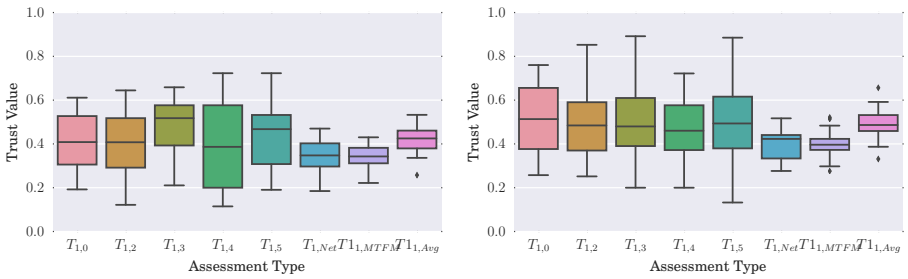
(c) All nodes but n_1 Random Walk (d) All Nodes Mobile

Fig. 3: Throughput/Delay Characteristics for varying node separations across increasing packet emission rates

context of Grey Relational Coefficient generation (2), the best sequence g was selected using the lowest PLR, delay, and powers, and the highest throughputs, with the worst sequence, b the inverse of these.

The particular factors under discussion are the relative performance of MTFM against OTMF and Beta with respect to statistical stability across mobilities and in responsiveness to changing network behaviour. We establish a similar result set by initially tracking the resultant trust values established by MTFM in each of the four mobility scenarios, shown in Fig.4. For simplicity, we are primarily concerned with the observational trust relationship between node 0 and node 1, i.e. n_0's assessment of the trustworthiness of n_1, or $T_{1,0}$. We are also concerned with the opinions of n_1 provided to n_0 by other nodes, where $[T_{1,2}, T_{1,3}]$ and $[T_{1,4}, T_{1,5}]$ denote the sets of recommendation and indirect trust assessment respectively. We also include a set aggregate assessments; $T_{1,\text{avg}}$, the flat average of direct trust assessments of n_1, $T_{1,\text{Net}}$, an aggregate that weights assessments according to the network topology from (7), and $T_{1,\text{MTFM}}$, the final MTFM trust assessment value based on both network topology and whitenisation from (6).

As expected, the variability in assessment is loosely tied to the mobility; in the static case (Fig. 4a), we see that the nodes close to n_1 ($[n_0, n_2, n_3]$) have reasonably consistent distributions, and as the range increases out to $[n_4, n_5]$, this variability increases. In the full mobility case, shown in Fig. 4b, this subjective variability is greatly increased, as the topology is highly dynamic and, as we'll discuss, delays on re-establishing routes are extremely volatile, perturbing the trust value. The aggregate trust values utilising the topology information ($T_{1,\text{Net}}, T_{1,\text{MTFM}}$) display a greatly decreased variation than those of the individual subjective observations in both cases.



(a) All Nodes Static (b) All Nodes Randomly Walking

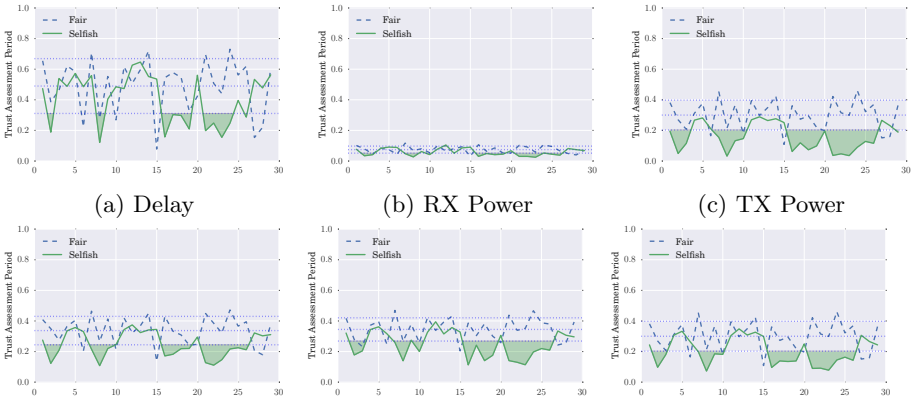
Fig. 4: MTFM Trust assessments for varying mobility options in the fair case

5.1 Weight Generation

For an arbitrary metric weight vector H, where the metric m_j is emphasised as being twice as important as the other metrics, we form an initial weighting

vector $H' = [1, 1, 1, 1, 2, 1]$ for $j = 4$ for example. We then scale that vector H' such that $\sum H = 1$ by $H = \frac{H'}{\sum H'}$.

Using this process we can extract and highlight the primary aspects of an attack by comparing against the deviation from the 'fairness' set by other nodes in the network;



(a) Delay (b) RX Power (c) TX Power

(d) RX Throughput (e) TX Throughput (f) PLR

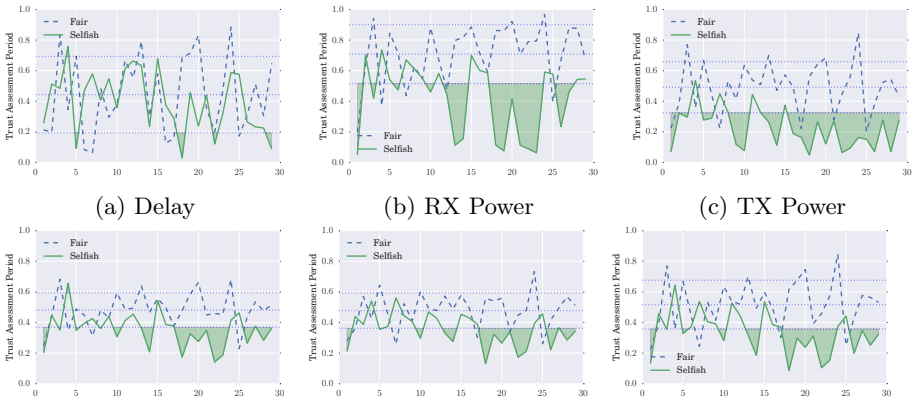
Fig. 5: $T_{1,0}$ in the Single Mobile case for the Bad Mouthing Power Control behaviour, emphasising a different metric in turn, also showing the mean and $\pm\sigma$ of the fair assessment

5.2 Comparison to OTMF and Beta

The same experiments were also performed utilising OTMF and Beta assessment as well as MTFM, providing like-for-like comparison of assessment at runtime.

It is important to note a distinction between the expectations of MTFM compared to other trust assessment frameworks; MTFM is primarily concerned with the identification of malicious or mistaken behaviours, and is relativistic in it's operation. That is to say that under Grey Theory, agents are compared against the worst current performances across metrics of other nodes and graded against them. OTMF and Beta in comparison are absolutist in their approach, and do not factor in a comparative metric for assessment; in the Bayesian book, you are good or bad regardless of what everyone else is doing. This relativistic versus absolutist differential is particularly stark when comparing mobility models.

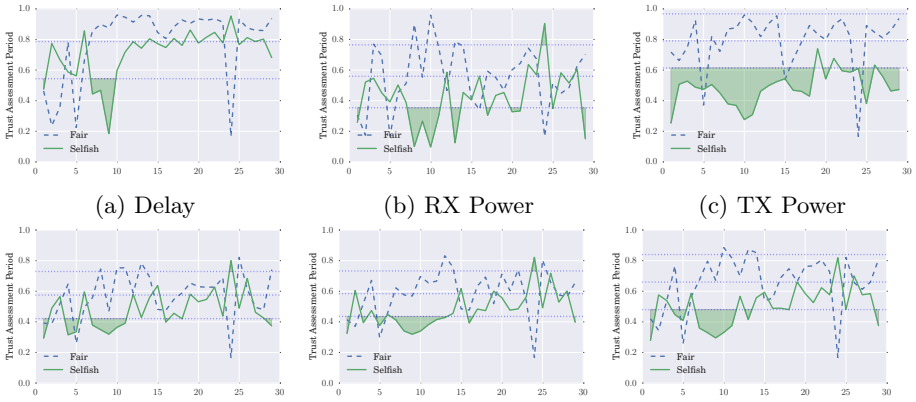
MTFM keeps a steady assessment that the node under assessment, n_1, is behaving "OK" regardless of mobility model. However, the network itself is most under strain with full mobility, with the routing topology changing every few minutes, requiring route advertisements and request overheads that contend the already valuable channel.



(a) Delay (b) RX Power (c) TX Power

(d) RX Throughput (e) TX Throughput (f) PLR

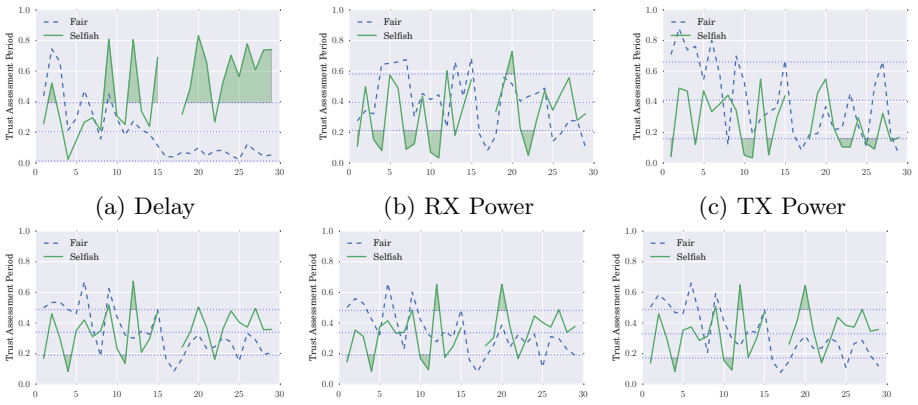
Fig. 6: $T_{1,0}$ in the Single Mobile case for the Bad Mouthing Power Control behaviour



(a) Delay (b) RX Power (c) TX Power

(d) RX Throughput (e) TX Throughput (f) PLR

Fig. 7: $T_{1,0}$ in the All-but-n_1 Mobile case for the Bad Mouthing Power Control behaviour



(a) Delay (b) RX Power (c) TX Power

(d) RX Throughput (e) TX Throughput (f) PLR

Fig. 8: $T_{1,0}$ in the All Mobile case for the Bad Mouthing Power Control behaviour

Another difference is that computationally, MTFM is significantly more intensive than the relatively simple Beta / OTMF implementation, and the repeated metric matrix re-weighting required for reasonable behaviour detection is an area that requires work for it's optimisation.

As such, a hybrid system could be implemented, that used OTMF as a 'trigger' to detect potentially selfish or malicious behaviour, and allow MTMF to be triggered at less regular intervals.

5.3 Comparison under malicious behaviour

Introducing a malicious actor into a trusted network with the aim to identifying the actor and the form of the malicious action is the driving force behind this work. Guo introduces a range of malicious actors, including modification of the packet loss rate of routing nodes and limiting throughput on a per-link basis as well as a selection of combined misbehaviours.

In all cases, the malicious node is n_1, the node that n_1 is "attacking" is $n0$, who is also the primary observer, e.g. the value of trust under assessment is $T_{0,1}$

- *Single Metric Misbehaviours*
  - *Packet Loss Rate*: n_1 selectively denies n_0's packets to reduce n_0's apparent PLR from the perspective of the rest of the network.
  - *Signal Strength*: n_1 increases it's standard operating signal strength for all nodes *except* communications with n_0.
  - *Delay*: n_1 introduces artificial delays to it's communications with n_0
  - *Throughput*: n_1 artificially prioritises or de-prioritises it's communications with n_0 above/below everyone else so n_0 appears to be behaving unfairly.

Given that the established links are already heavily constrained, heavy handed attacks such as introducing selective PLR and adding to the already extreme and hugely variable delays would severely impact the general performance of the network beyond the scope of simple selfishness, effectively triggering saturation collapses in regions that the network should be stable.

In the interests of investigating the operation of trust and not of the network, we select a Signal Strength attack for n_1 to perpetrate on n_0, where n_1 increases it's own transmission power to everyone else.

The use of Forward Beam Routing and a RTS/CTS MACA MAC scheme from AUVNetSim in our particular simulation mitigate a significant number of potential packet losses through collision avoidance, leading to the situation that the only genuinely lost packets occur when a node wanders completely out of range of any other node, and given the scenario constraints in [5], this is not likely in our scenario until increasing separation beyond 500-600m

A significant factor of trust assessment in such a constrained environment is that there may be long periods where two edge nodes (for instance, $n0 \rightarrow n_5$) may not interact at all. This can be due to a range of factors beyond potential malicious behaviour including simple random scheduling coincidence, and intermediate or neighbouring nodes collectively causing long back-off or contention periods. This disconnection hinders and skews trust assessment in two ways; assessing nodes who do not receive timely recommendations may make decisions based on very old data, and malicious nodes have a long dwelling time where they can operate under a reasonable certainty that the TMF will not detect it (especially if it itself is performing disruptive routing attacks). One potential solution to this would be to move from a stepping-window of trust periods to a continuous trust log, updated on packet reception rather than waiting for a reasonable number of packets to arrive.

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. Also remember to show the RTS ratio for the mobility case, highlighting that when the environment is significantly more dynamic and delay tolerant, beta/otmf fail to take that into account.

select metrics

6 Conclusions and Future Work

We have demonstrated that existing MANET Trust Management Frameworks cannot be directly applied to the contentious and dynamic underwater medium. With significant delays (order from seconds to hours), a fading, refractive medium with varying propagation, the environment is simply not as predictable as classical MANET deployment environments.

We presented a comparison scenario between trust establishment in Terrestrial MANET and in the underwater space, demonstrating that in order to have any reasonable expectation of performance, throughput and delay responses must be characterised before implementing trust in such environments.

We demonstrated initial, unfiltered Grey Trust assessment utilising all the available metrics (transmitted and received throughput, delay, received signal strength, transmitted power, and packet loss rate) Using the knowledge that in a 'fair' environment, trust assessments should be stable about 0.5, selected THESE to continue.

We have shown that existing frameworks are overly optimistic [6] 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

Acknowledgments. The Authors would like to thanks the UK/FR DSTL PhD Programme for their support during this project.

7 The References Section

References

1. Sonja Buchegger and Jean-Yves Le Boudec, *Performance analysis of the CONFIDANT protocol*, Proc. 3rd ACM Int. Symp. Mob. ad hoc Netw. Comput. - MobiHoc '02 (2002), 226–236.
2. Andrea Caiti, *Cooperative distributed behaviours of an AUV network for asset protection with communication constraints*, Ocean. 2011 IEEE-Spain (2011).
3. Jin-hee Cho, Ananthram Swami, and Ing-ray Chen, *A survey on trust management for mobile ad hoc networks*, Commun. Surv. & Tutorials **13** (2011), no. 4, 562–583.
4. Ji Guo, *Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks*, (2012).
5. Ji Guo, Alan Marshall, and Bosheng 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 (2011), 142–149.
6. Dijiang Huang, Xiaoyan Hong, and M Gerla, *Situation-aware trust architecture for vehicular networks*, Commun. Mag. IEEE (2010), no. November, 128–135.
7. Huaizhi Li and Mukesh Singhal, *Trust Management in Distributed Systems*, Computer (Long. Beach. Calif). **40** (2007), no. 2, 45–53.
8. Jie Li, Ruidong Li, Jien Kato, Jie Li, Peng Liu, and Hsiao-Hwa Chen, *Future Trust Management Framework for Mobile Ad Hoc Networks*, IEEE Commun. Mag. **46** (2007), no. 4, 108–114.
9. K J R Liu, *Information theoretic framework of trust modeling and evaluation for ad hoc networks*, IEEE J. Sel. Areas Commun. **24** (2006), no. 2, 305–317.
10. Junhai Luo, Xue Liu, Yi Zhang, Danxia Ye, and Zhong Xu, *Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks*, 2008 33rd IEEE Conf. Local Comput. Networks (2008), 305–311.
11. Josep Miquel and Jornet Montana, *AUVNetSim: A Simulator for Underwater Acoustic Networks*, Program (2008), 1–13.
12. MEG E G Moe, BE E Helvik, and SJ J Knapskog, *TSR: Trust-based secure MANET routing using HMMs*, . . . Symp. QoS Secur. . . . (2008), 83–90.
13. Klaus Müller and Tony Vignaux, *SimPy: Simulating Systems in Python*, ONLamp.com Python DevCenter (2003).
14. Jochen Mundinger and JY Le Boudec, *Analysis of a reputation system for mobile ad-hoc networks with liars*, Perform. Eval. (2008), 0–5.
15. David K W Ng, *Grey System and Grey Relational Model*, SIGICE Bull. **20** (1994), no. 2, 2–9.

16. Jim Partan, Jim Kurose, and Brian Neil Levine, *A survey of practical issues in underwater networks*, Proc. 1st ACM Int. Work. Underw. networks WUWNet 06 **11** (2006), no. 4, 17.
17. Andrej Stefanov and Milica Stojanovic, *Design and performance analysis of underwater acoustic networks*, IEEE J. Sel. Areas Commun. **29** (2011), no. 10, 2012–2021.
18. Milica Stojanovic, *On the relationship between capacity and distance in an underwater acoustic communication channel*, 2007, p. 34.
19. Y Wang, V Cahill, E Gray, C Harris, and L Liao, *Bayesian network based trust management*, Auton. Trust. . . . (2006), no. 60373057, 246–257.
20. Fengchao Zuo, *Determining Method for Grey Relational Distinguished Coefficient*, SIGICE Bull. **20** (1995), no. 3, 22–28.

Todo list