Assessment of TMF Performance in Marine Environments

Andrew Bolster

October 5, 2015

1 Comparison of Terrestrial and Marine Communication Trust Assessments

In this chapter, we demonstrate the need for multi-metric trust assessment in Underwater Autonomous Networks (UAN). Many UANs use MANET architectures, however the marine environment presents new challenges for trust management frameworks that have been developed for use in conventional (i.e. Terrestrial RF) MANETs. We investigate the operation of a selection of traditional MANET TMFs in this environment. We characterise these challenges and present results that demonstrate a multi-metric approach to Trust greatly enhances the effectiveness of TMFs in these environments.

1.1 Trust in Marine Networks

With 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 the benefits they present are significant. Beyond the constraints of the communications environment, knock on pressures are applying in battery capacity, on-board processing, and locomotion. These pressures simultaneously present opportunities and incentives for malicious or selfish actors to appear to cooperate while not reciprocating, in order to conserve power for instance. These multiple aspects of potential incentives, trust, and fairness do not directly fall under the scope of single metric trusts discussed above, and this context indicates that a multi-metric approach may be more appropriate.

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 to different communications environments to ensure their continued security, reliability, and performance.

One area of application is the underwater marine environment, where extreme challenges to communications present themselves (propagation delays, frequency dependent attenuation, fast and slow fading, refractive multi-path

distortion, etc.). In addition to the communications challenges, other considerations such as command and control isolation, as well as power and locomotive limitations, drive towards the use of teams of smaller and cheaper autonomous underwater vehicles (AUVs). These increasingly decentralised applications present unique threats against trust management [**?**]. In underwater environments, communications is both sparse and noisy. Therefore the observations about the communications processes that are used to generate the trust metrics, occur much less frequently, with much greater error (noise) and delay than is experienced in terrestrial RF MANETS. As such, the use of trust methods developed in the terrestrial MANET space must be re-appraised for application within the underwater context [**?**].

Trust Management Frameworks (TMFs) provide information to assist the estimation of future states and actions of nodes within networks. This information is used to optimize the performance of a network against malicious, selfish, or defective misbehaviour by one or more nodes. Previous research has established the advantages of implementing TMFs in 802.11 based MANETs, particularly in terms of preventing selfish operation in collaborative systems [**?**], and maintaining throughput in the presence of malicious actors [**?**]

Most current TMFs use a single type of observed action to derive trust values, typically successfully delivered or forwarded packets. These observations then inform future decisions of individual nodes, for example, route selection [**?**].

Recent work has demonstrated the use of a number of metrics to form a "vector" of trust. The Multi-parameter Trust Framework for MANETs (MTFM) [**?**], uses a range of communications metrics beyond packet delivery/loss rate (PLR) to assess trust. This vectorized trust also allows a system to detect and identify the tactics being used to undermine or subvert trust. To date this work has been limited to terrestrial, RF based networks.

1.2 Establishing Scale Factors in Communications Rate

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

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. **??** and 2, 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. 2, 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 in the small static case.

Figure 1: Varying packet emission rate demonstrates maximal throughput at 0.025 packets per second, equivalent to ≈240 bps

Figure 2: Varying packet emission rate demonstrates a saturation point at 0.025 packets per second

1.3 Establishing Scale Factors in Physical Distribution

In this section we characterise the effect of node-separation scaling on communications operation for comparison against [**?**]. 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 **??**, the operating transmission range of acoustic 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. Therefore, a reasonable experimental range would have an upper bound of performance around this scaling factor, where nodes are approximately $400m$ apart.

A reasonable range around this is to scale from $100m$ apart on average to $800m$.

Varying average node separation shows that while direct throughput isn't significantly affected until, collision rates are Fig. 3. This collision rate is well within the tolerances of the MAC layer, as shown in Fig. 4, where even with a rising collision rate, packets are being reliably received.

Figure 3: Comparison of Medium Acquisition Collisions, Throughput, and Enqueued packets against varying application packet emission rates.

Figure 4: Probability of Timely Reception across a range of node scaling.

However, when end-to-end delay is investigated, it's clear from Fig. 5 that the network is becoming severely impaired approaching the $600m$ mark, with delays rising to more than 25 minutes above $700m$. This is also demonstrated by the increasing RTS/Data ratio shown in Fig. 6.

According to Xu [**?**], 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. 6, 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.

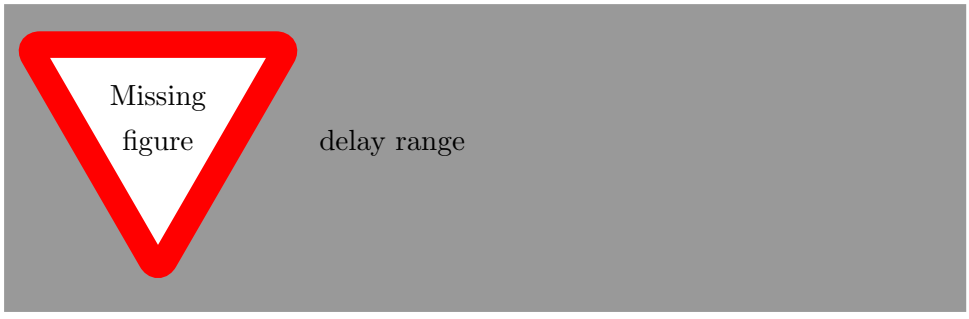

Figure 5: End to End Delay under varying node-separations

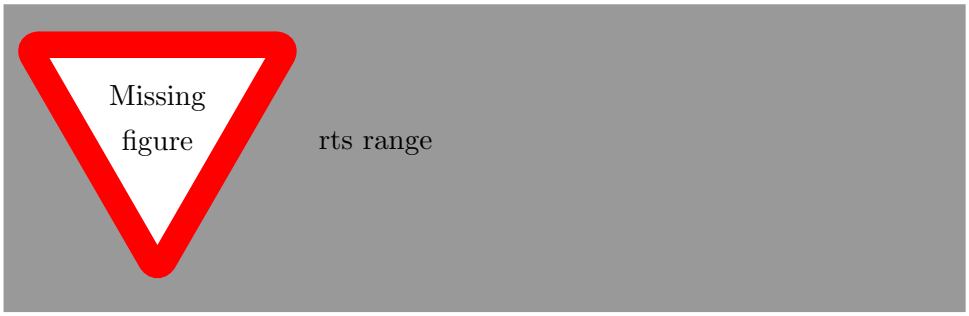

Figure 6: RTS/Data ratio for varying node-separations

Table 1: Tabular view of data from Figs 4, 5, and 6

Separation(m)	Delay(s)	Probability of Arrival	RTS/Data Ratio	Ideal Delivery Time(s)
100	60.32	0.99	1.80	1.03
200	419.95	0.97	2.02	1.10
300	1205.66	0.89	2.41	1.17
400	1288.20	0.91	2.26	1.25
500	1868.20	0.87	2.41	1.32
600	2191.07	0.85	2.42	1.39

References

[] Sonja Buchegger and Jean-Yves Le Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc '02*, pages 226–236. ACM Press, 2002.

[] Andrea Caiti. Cooperative distributed behaviours of an AUV network for asset protection with communication constraints. *OCEANS, 2011 IEEE-Spain*, 2011.

[] 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. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Sys-*

tems, ICESS 2011, 6th Int. Conf. on FCST 2011, pages 142–149, 2011.

[] Jie Li, Ruidong Li, Jien Kato, Jie Li, Peng Liu, and Hsiao-Hwa Chen. Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Communications Magazine*, 46(4):108–114, April 2007.

[] Huaizhi Li and Mukesh Singhal. Trust Management in Distributed Systems. *Computer*, 40(2):45–53, 2007.

[] Surya Pavan, Kumar Gudla, and N Preeti. An Overview of Reputation and Trust in Multi Agent System in Disparate Environments. 5(3):498–504, 2015.

[] Kaixin Xu, Mario Gerla, Sang Bae, and Hoc Networks. Effectiveness of RTS / CTS Handshake in IEEE. *. . . , 2002. Globecom'02. Ieee*, 56:1–14, 2002.