Single and Multi-Metric Trust Management Frameworks for use in Underwater Autonomous Networks

Andrew Bolster and Alan Marshall

University of Liverpool

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

Recent Advances of Trust, Security and Privacy in Computing Communications (RATSP)

Motivation

- Related Work
- Challenges to Trust in Underwater Networks

Our Contribution

- Experimental Context
- MTFM Operation
- Single vs Multi
- Metric Weighting
- Metric Significance
- Current Work

Summary

- Trust Methods in the MANET space applied to other arenas (e.g. underwater acoustics).
- These Trust Management Frameworks (TMFs) require reassessment to work the sparse, noisy and contested marine communications environment.
- Most rely on one[1]type of observation (metric)
- Recent work (MTFM [1]) introduces the use of multiple types of continuous metrics for assessment.
- How do these Single and Multi-Metric Frameworks perform in the challenging marine communications environment?
- What metrics are suitable for use underwater?

[1]Packet Loss Rate (PLR) or other binary interaction success observation

Outline

- Motivation
  - Related Work
  - Challenges to Trust in Underwater Networks
- Our Contribution
  - Experimental Context
  - MTFM Operation
  - Single vs Multi
  - Metric Weighting
  - Metric Significance
  - Current Work

Trust in Conventional MANETS

- TMFs provide information to assist the estimation of future states and actions of nodes within networks.
- Centralised methods (CA/TTP/PKI) unsuitable for dynamic decentralised networks[2].
- Need to detect, identify, & mitigate threats in a distributed fashion.

Single-Metric TMFs I

- *Hermes* [3] - Bayesian estimation based on PLR; encapsulates both "Trust" and "Confidence")
- *OTMF* [4] - Collaborative Assessments of Bayesian Trust, PLR.
- *TSR* [5] - Builds HMM into Dynamic Source Routing (DSR), Session Loss Rate.
- *CONFIDANT* [6] - Probabilistic PLR assessment, includes some topology and reputational weighting.
- *Fuzzy Trust-Based Filtering* [7] - Fuzzy classification on the *nature* of packet delivery (eg. "late", "unreliable", "unknown", etc.)

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

Single-Metric TMFs II

- Single Metric TMFs present 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 (e.g. power, mobility, channel occupancy, physical location)

Multi-Metric TMF I

- *Multi-metric Trust For MANETS (MTFM)* [1] - Uses additional metrics such as Power, Throughput, Delay, etc. in addition to PLR to assess trust, as well as incorporating topological and metric weighting.
- Use of multiple metrics allows classification of behaviours through dynamic metric weighting.
- Use of Grey Relational Grading to provide dynamic runtime normalisation, assessing *comparative* trust within a cohort of actors.

Multi-Metric TMF II

$$\theta^t_{k,j} = \frac{\min_k |a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|}{|a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|} \tag{1}$$

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

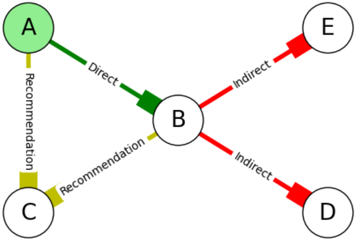
$$[\theta^t_k, \phi^t_k] = \left[\sum_{j=0}^{M} h_j \theta^t_{k,j}, \sum_{j=0}^{M} h_j \phi^t_{k,j}\right] \tag{3}$$

$$T^t_k = (1 + (\phi^t_k)^2/(\theta^t_k)^2)^{-1} \tag{4}$$

Where $a^t_{k,j}$ 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 $\{a^t_{k,j} k = 1, 2 \ldots K\}$, $H = [h_0 \ldots h_M]$ is a metric weighting vector such that $\sum h_j = 1$

Multi-Metric TMF III

This Grey Trust value is then combined[2] with the shared assessments from other actors in the network weighted based on their relative topology to provide a final value; $T_{i,j}^{MTFM}$



[2] ▸ Details

Multi-Metric Compared to Single in MANETs

Guo et al.[1] demonstrated that MTFM operates favourably in 802.11 based terrestrial MANETs against OTMF and Hermes, and can accurately detect, identify, & characterise misbehaviours within a group of six nodes, with n_0 as the primary observer and n_1 as the misbehaver.

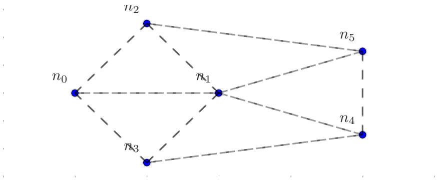


Fig. 1: Initial Node Layouts in [1]

Outline

Communications Channel Considerations I

Key Characteristics of the Marine Acoustic Channel [8, 9, 10, 11]:

- Slow propagation ($1400 ms^{-1}$) 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

Communications Channel Considerations II

The attenuation that occurs in an underwater acoustic channel over a distance d for a signal about frequency f in linear power is given as $A_{aco}(d, f) = A_0 d^k a(f)^d$ and in dB form as;

$$10 \log A_{aco}(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{5}$$

where A_0 is a normalising constant, k is a spreading factor (commonly taken as 1.5 [10]), and $a(f)$ is the absorption coefficient, approximated using Thorp's formula [11]

$$10 \log a(f) = \frac{0.11 \cdot f^2}{1 + f^2} + \frac{44 \cdot f^2}{4100 + f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{6}$$

Communications Channel Considerations III

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

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

Outline

Operational Considerations: Collaborative AUV Survey

Context:

- Fleets of up to 16 collaborating Autonomous Underwater Vehicles(AUVs)
- Constrained in Power, Mobility, Processing, Storage Capacity
- Tasked to perform ongoing survey of an area

Communications Efficiency is not the only operational asset at risk from malicious exploitation

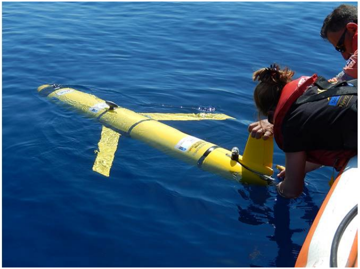


Fig. 2: REMUS 100 AUV as deployed at NATO CMRE La Spezia

Scale Considerations

- Simulations based on SimPy [12], Network stack using AUVNetSim [13] and channel constraints based on Stojaovic and Stefanov [10, 11] ▸ Details
- Established a safe operating zone in terms of communications rate and node distances to optimise for delay/throughput at 0.015pps and avg. init. range 300m ▸ Details
- Six per-link communications metrics: TX/RX Throughput/Power, Delay and PLR, lacking the 802.11 Data Rate metric from [1]

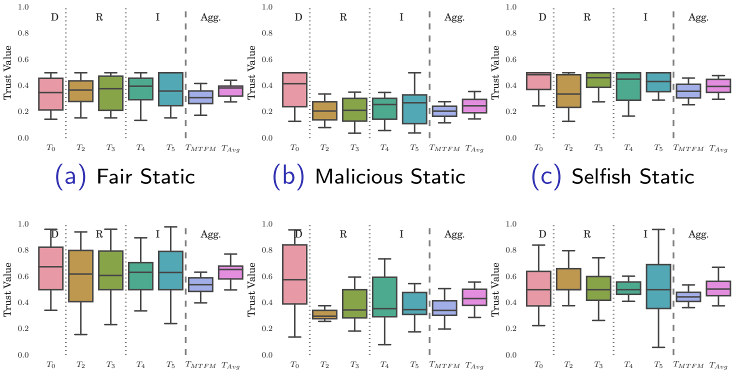
Misbehaviour Specification

Two misbehaviours developed:

- *Malicious Power Control*(MPC) - attacker n_1 aims to make n_0 appear selfish by increasing power to all nodes except to/from n_0
- *Selfish Target Selection*(STS) - n_1 preferentially communicates with nodes close to it, to conserve its own power.

Outline

Multi-Metric Operation I



(a) Fair Static (b) Malicious Static (c) Selfish Static

(d) Fair Mobile (e) Malicious Mobile (f) Selfish Mobile

Fig. 3: Observations of n_1 ($T_{1,X}$), showing Direct, Recommender and Indirect relationships and T_{MTFM} and T_{AVG} Closeup

Multi-Metric Operation II

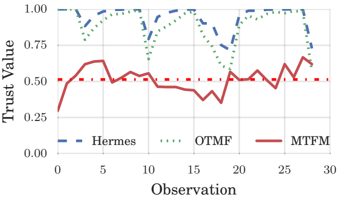
Key Observations:

- Mobility greatly increases variation in instantaneously observed trust
- T_{MTFM} remains more stable in both mobility cases when compared to either single-node assessments or T_{Avg}
- Raw T_{MTGM} isn't perfect; in Fig 6e demonstrates huge variability in Direct assessment ($T_{1,0}$) that isn't reflected in T_{MTFM}. Partially expected in this directed attack.
- Larger general variability in observations in "Fair" case compared to misbehaviours

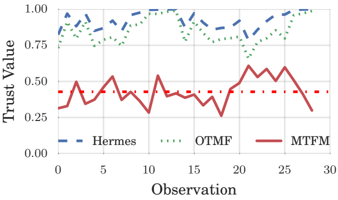
Outline

Blind Comparison of Single/Multi-metric TMFs

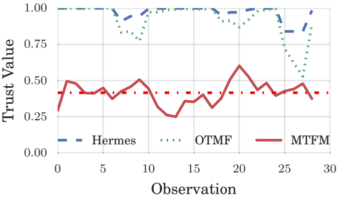
Blind Comparison of Single/Multi-metric TMFs I



(a) Fair Scenario



(b) Malicious Power Control Scenario



(c) Selfish Target Selection Scenario

$T_{1,0}$ for Hermes, OTMF and MTFM assessment values for fair and malicious behaviours in the fully mobile scenario (mean of MTFM also shown)

Blind Comparison of Single/Multi-metric TMFs II

Key Observations:

- Neither misbehaviour, while impacting network fairness, directly affects PLR
- MTFM's Cohort Comparison means in the fair case, 0.5 is expected
- In OTMF/Hermes, T 1 is expected
- Neither OTMF, Hermes or Blind MTFM are particularly effective
- MTFM indicates 10% selectivity between Fair and Either Misbehaviour

Outline

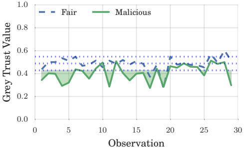
Metric Weighting

From 3, metric emphasise can be adjusted, highlighting misbehaviour in particular metric areas

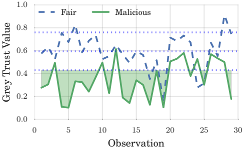
$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t\right] \tag{7}$$

$$T_k^t = (1 + (\phi_k^t)^2 / (\theta_k^t)^2)^{-1} \tag{8}$$

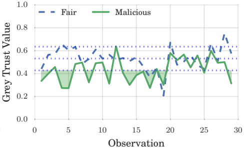
Malicious Power Control - Weighted Emphasis



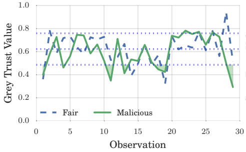
(a) Delay Emphasised



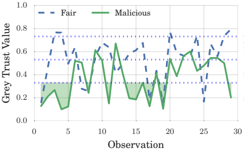
(b) PLR Emphasised



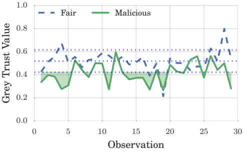
(c) RX Power Emphasised



(d) TX Power Emphasised



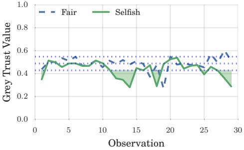
(e) RX Throughput Emphasised



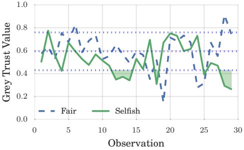
(f) TX Throughput Emphasised

Fig. 4: $T_{1,MTFM}$ in the All Mobile case for the Malicious Power Control behaviour, including dashed $\pm\sigma$ envelope about the fair scenario ▸ Closeup

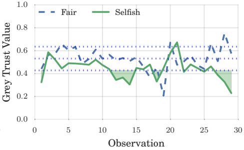
Selfish Target Selection - Weighted Emphasis



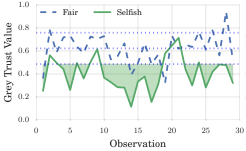
(a) Delay Emphasised



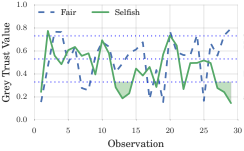
(b) PLR Emphasised



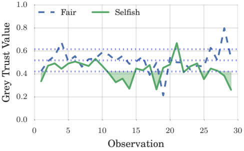
(c) RX Power Emphasised



(d) TX Power Emphasised



(e) RX Throughput Emphasised



(f) TX Throughput Emphasised

Fig. 5: $T_{1,MTFM}$ in the All Mobile case for the Selfish Target Selection behaviour, including dashed $\pm\sigma$ envelope about the fair scenario ▸ Closeup

Metric Weighting

Key Observations:

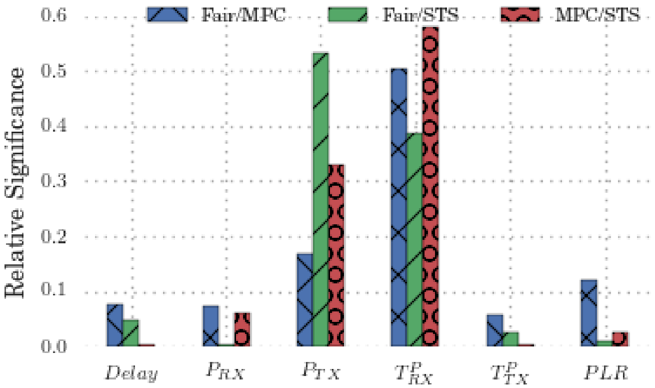
- In MPC case:
  - Consistently outside $\pm\sigma$ in all but P_{TX}, particularly PLR
  - Less so in Delay, P_{RX} and T_{TX}
- In STS case:
  - Less overall impact, except when P_{TX}
- In General:
  - Qualatatively similar to similar experiments performed in [1] in RF Terrestrial MANET
  - Lower differences between misbehaviour/fair cases
  - Less consistent deviations
  - More useful than OTMF/Hermes but still not perfect

Outline

Regression of Metric Significance I

- Distributed Random Forest Regression [14]
- 729 Metric Weight Vectors (H), 512 random trees
- 16 Random starts of each of the 3 scenarios for 6 nodes for 6 hour "missions"
- Targeting area of $\pm\sigma$ deviation $\int abs(T_m - \overline{T}_f) - \sigma_{T_f}$
- Regression identifies the significance of metrics in classifying between the three possible behaviours

Regression of Metric Significance II



Correlation	Delay	P_{RX}	P_{TX}	T^P_{RX}	T^P_{TX}	PLR
Fair / MPC	0.199	0.159	-0.416	0.708	-0.238	-0.401
Fair / STS	0.179	-0.009	0.724	-0.697	-0.145	-0.052
MPC / STS	0.058	-0.134	0.146	-0.768	0.052	0.146

Regression of Metric Significance III

Key Observations:

- PLR not necessarily the most important metric
- Combination of Significance and Correlations demonstrate selectivity opportunity
- MTFM has capability to finely discriminate between similar misbehaviours
- PLR impact is minimal in STS, would not be detected by OTMF/Hermes even in less sparse/harsh environment
- Identifying this classification "comb" is computationally intensive and grows exponentially with number of metrics involved for brute force regression

Outline

Current Work and Paths to Proof/Implementation

- Include Physical Observations in Metric Set
  - Assess benefits / drawbacks of domain separation / joining
  - Assess complexity vs selectivity of derived classifications
- Perform / Initiate practical trials in collaborations with NATO CMRE

Summary

- Trust Underwater is Hard, but it's mostly the environments' fault
- Single-Metric Trust is unstable in such an environment
- Multi-Metric Trust works and can discriminate between behaviours
- Not all metrics are equally useful

- Outlook
  - Extending to include Physical Metrics
  - Developing runtime heuristics to improve complexity
  - Perform untrained classification performance on real data

References I

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.

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%5C_all.jsp?arnumber=6003463.

References II

- 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.
- 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%5C_all.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: *. . . Symp. 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* (2002), pp. 226–236. DOI: 10.1145/513800.513828. URL: http://dl.acm.org/citation.cfm?id=513800.513828.

References IV

- 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.
- R J Urick. *Principles of underwater sound*. 1983, NewYork.423pages.
- 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.

References V

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/~millitsa/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.

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 VI

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.

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.

The End

Grey Trust Equs I

Add backlinks

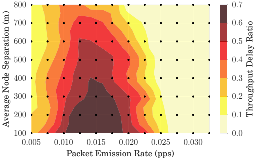
$$
\begin{aligned}
T_{i,j}^{MTFM} =& \frac{1}{2} \cdot \max_{s}\{f_s(T_{i,j})\} T_{i,j} \\
&+ \frac{1}{2} \frac{2|N_R|}{2|N_R| + |N_I|} \sum_{n \in N_R} \max_{s}\{f_s(T_{i,n})\} T_{i,n} \\
&+ \frac{1}{2} \frac{|N_I|}{2|N_R| + |N_I|} \sum_{n \in N_I} \max_{s}\{f_s(T_{i,n})\} T_{i,n}
\end{aligned} \tag{9}
$$

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...

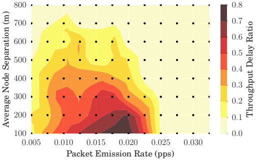
Grey Trust Equs II

$$
\begin{aligned}
f_1(x) &= -x + 1 \\
f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\
f_3(x) &= x
\end{aligned}
\tag{10}
$$

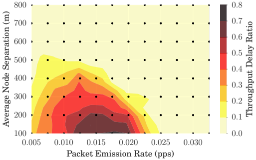
Comms Scaling Graphs I



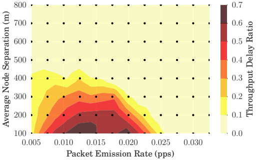
(a) All Nodes Static



(b) n_1 Random Walk



(c) All nodes but n_1 Random Walk



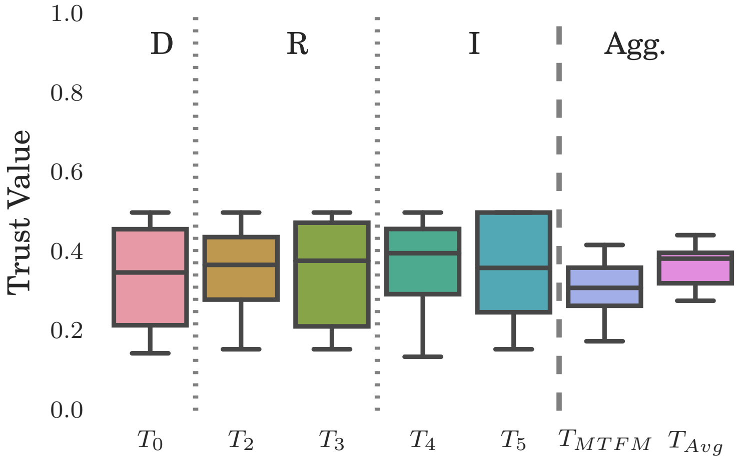
(d) All nodes Random Walk

System Model Constraints

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

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

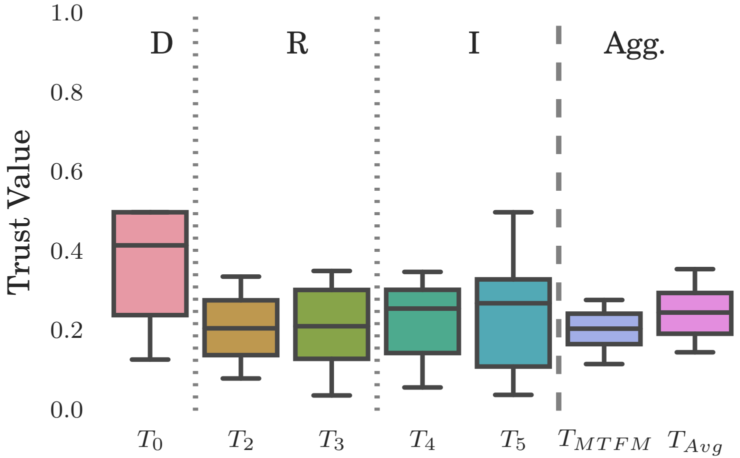
MTFM Operation Detail



(a) Fair Static

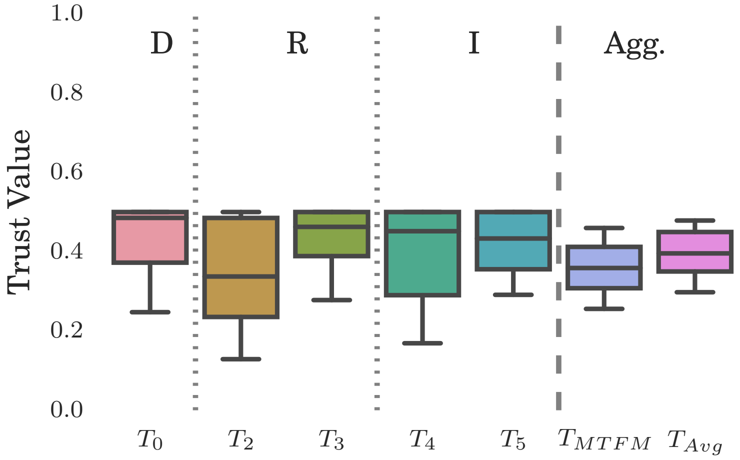
Add backlinks

MTFM Operation Detail



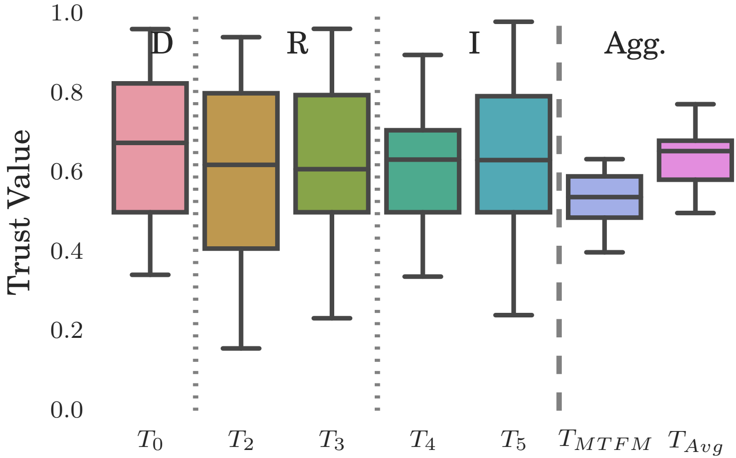
(b) Malicious Static

MTFM Operation Detail



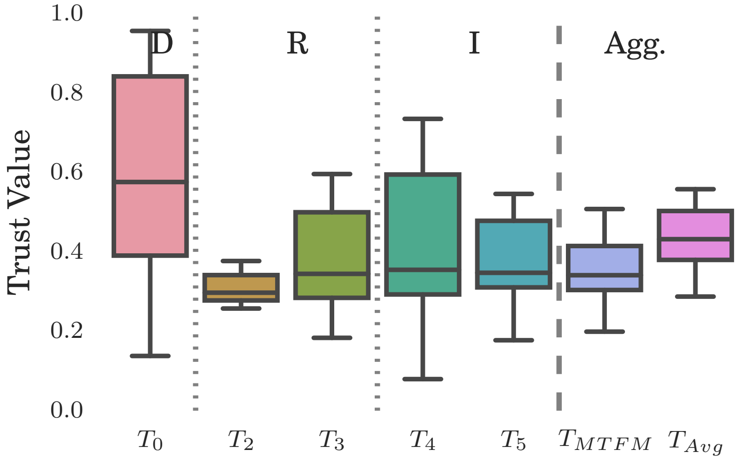
(c) Selfish Static

MTFM Operation Detail



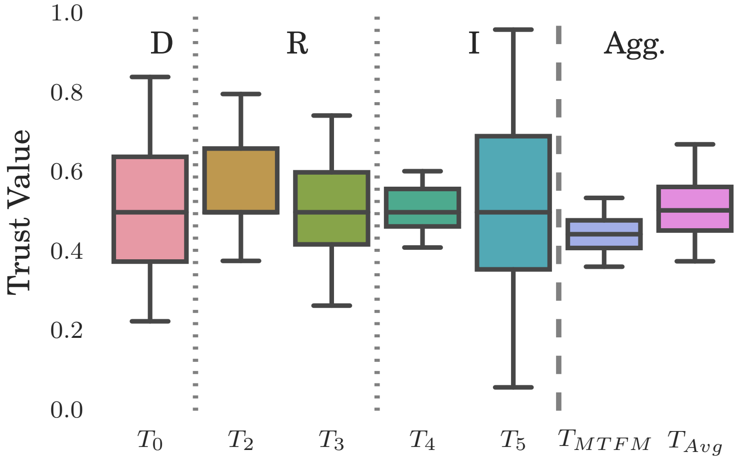
(d) Fair Mobile

MTFM Operation Detail



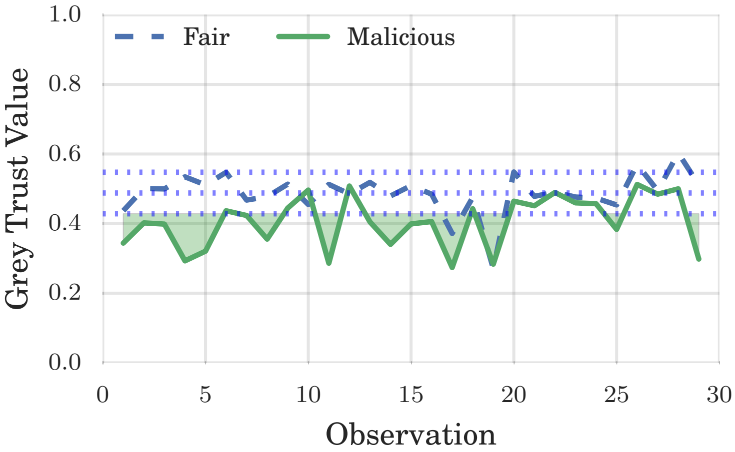
(e) Malicious Mobile

MTFM Operation Detail



(f) Selfish Mobile

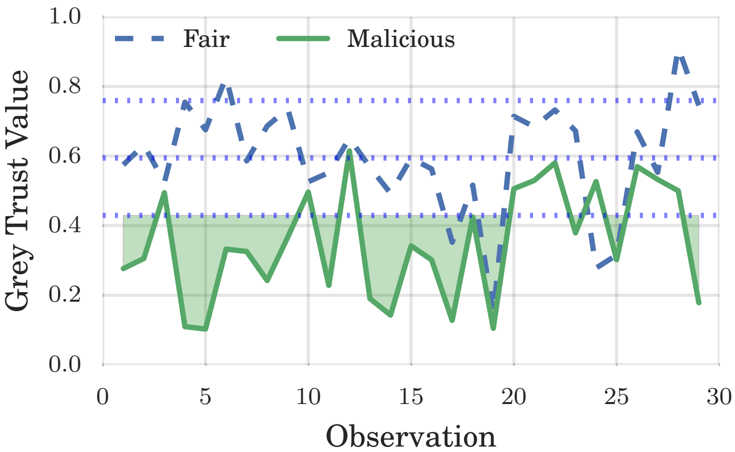
MTFM Malicious Power Control Detail



(a) Delay Emphasised

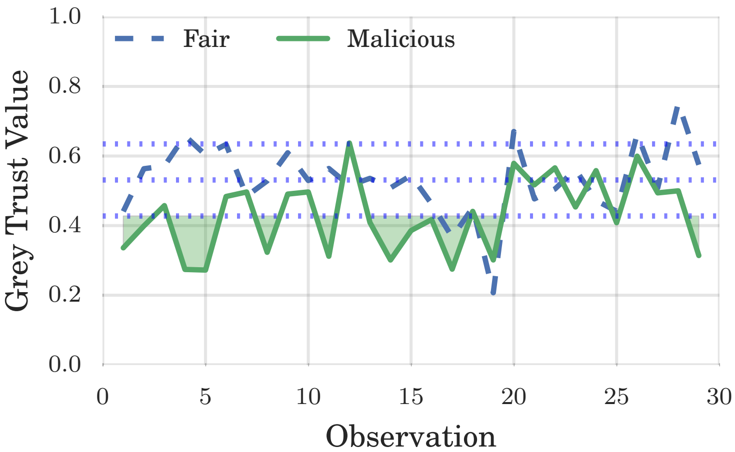
Add backlinks

MTFM Malicious Power Control Detail



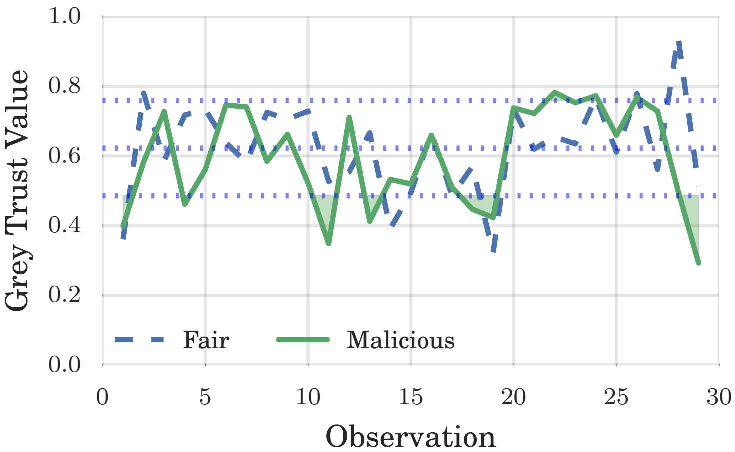
(b) PLR Emphasised

MTFM Malicious Power Control Detail



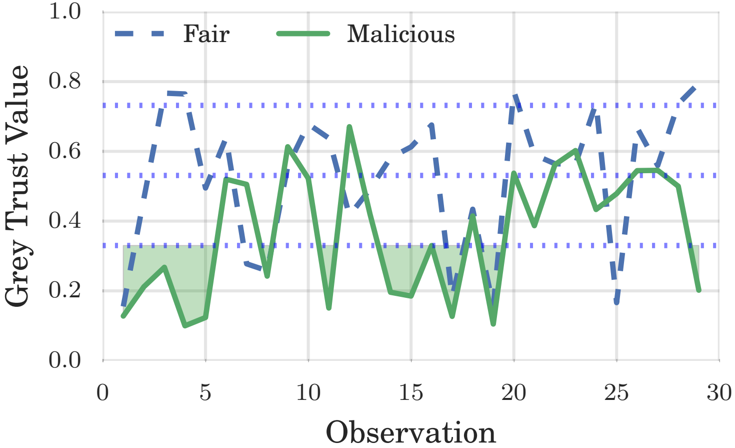
(c) RX Power Emphasised

MTFM Malicious Power Control Detail



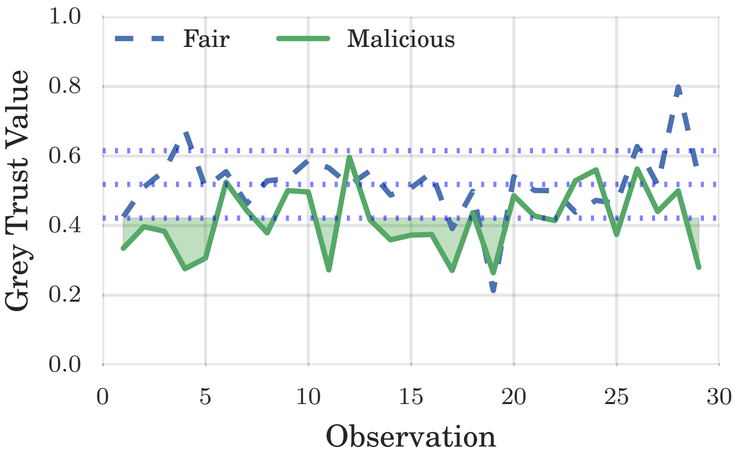
(d) TX Power Emphasised

MTFM Malicious Power Control Detail



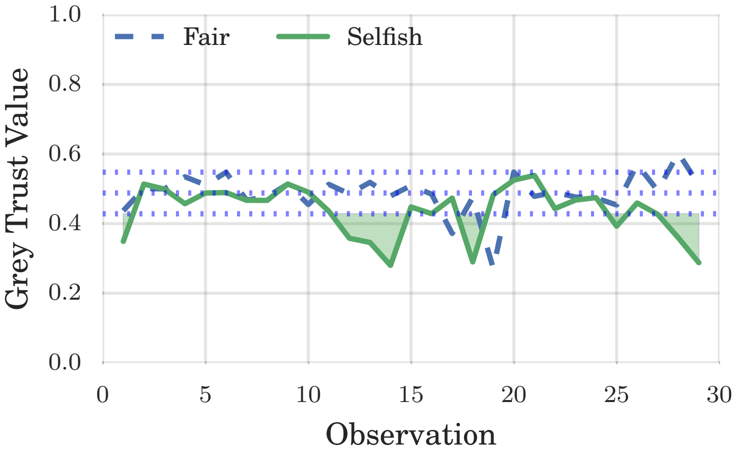
(e) RX Throughput Emphasised

MTFM Malicious Power Control Detail



(f) TX Throughput Emphasised

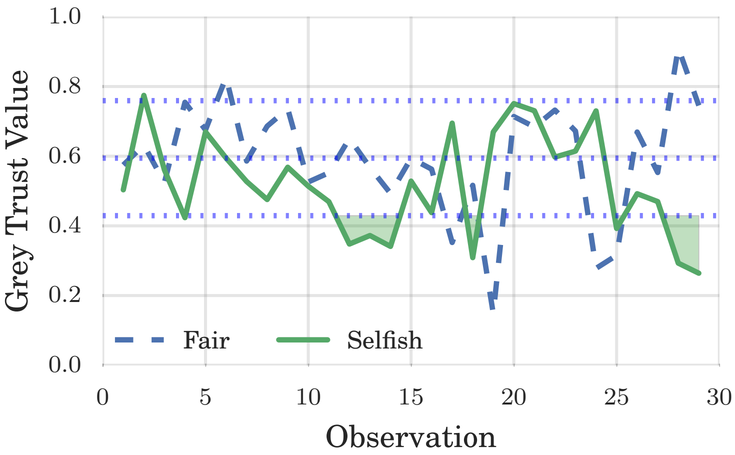
MTFM Selfish Target Selection Detail



(a) Delay Emphasised

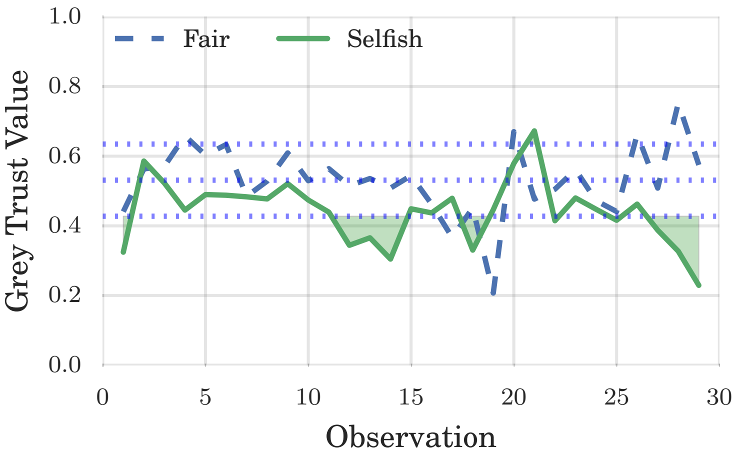
Add backlinks

MTFM Selfish Target Selection Detail



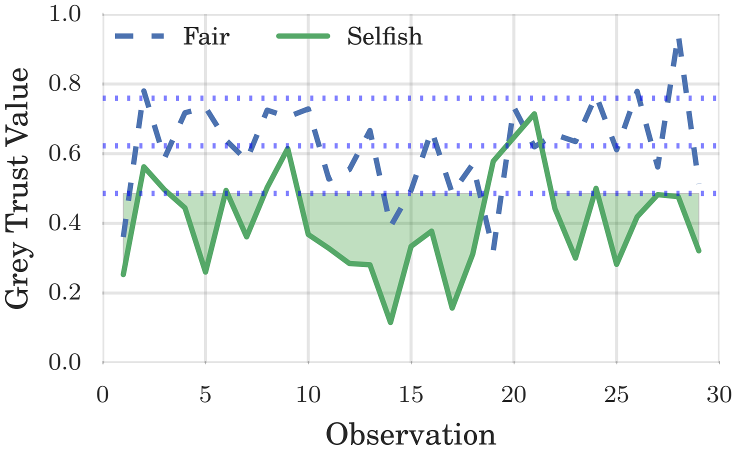
(b) PLR Emphasised

MTFM Selfish Target Selection Detail



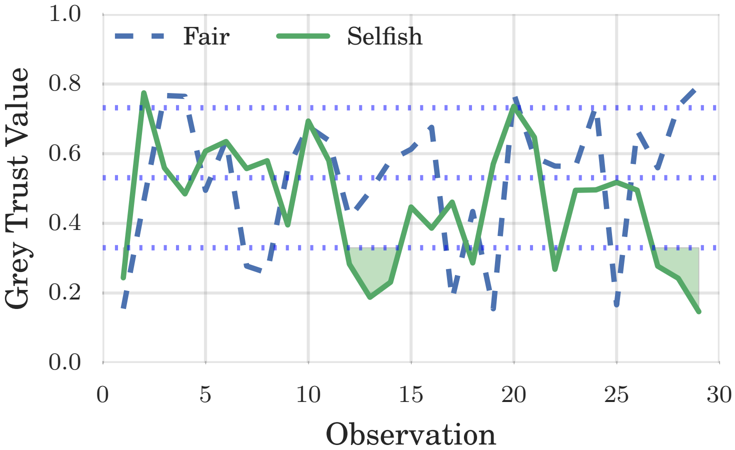
(c) RX Power Emphasised

MTFM Selfish Target Selection Detail



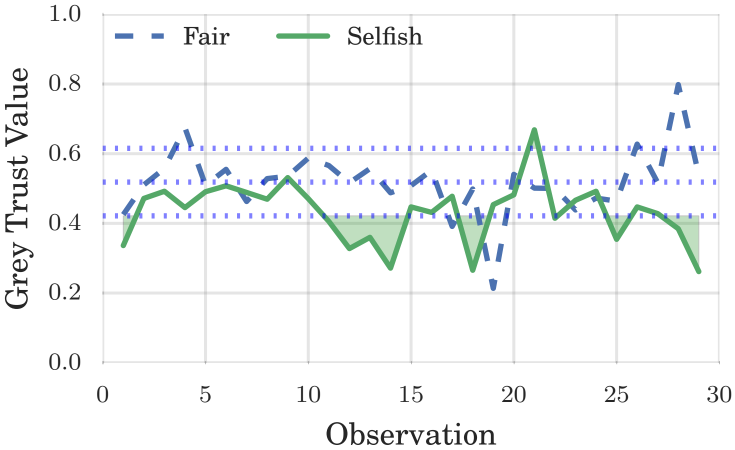
(d) TX Power Emphasised

MTFM Selfish Target Selection Detail



(e) RX Throughput Emphasised

MTFM Selfish Target Selection Detail



(f) TX Throughput Emphasised