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

UNIVERSITY OF LIVERPOOL

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

Summary

- Trust Methods in the MANET space applied to other arenas (e.g. underwater acoustics).
- Trust Management Frameworks (TMFs) require reassessment to work in the harsh marine communications environment.
- Most rely on one type of observation (metric)
- Recent work[1] introduces the use of multiple types of continuous metrics for assessment.

Summary

- Trust Methods in the MANET space applied to other arenas (e.g. underwater acoustics).
- Trust Management Frameworks (TMFs) require reassessment to work in the harsh marine communications environment.
- Most rely on one type of observation (metric)
- Recent work[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?

Outline

Trust in Conventional MANETS

- TMFs provide information to assist the estimation of future states and actions of nodes within networks.

Trust in Conventional MANETS

- TMFs provide information to assist the estimation of future states and actions of nodes within networks.
- Centralised methods unsuitable for dynamic networks in terms of efficiency and robustness.[2]

Trust in Conventional MANETS

- TMFs provide information to assist the estimation of future states and actions of nodes within networks.
- Centralised methods unsuitable for dynamic networks in terms of efficiency and robustness.[2]
- Need to detect, identify, & mitigate threats in a distributed fashion.

Single-Metric TMFs I

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

- *Hermes*[3] - Bayesian estimation based on PLR
- *OTMF*[4] - Collaborative Bayesian Trust
- *TSR*[5] - HMM route assessment, Session Loss Rate.
- *CONFIDANT*[6] - Probabilistic PLR assessment, includes topology and reputation weighting.
- *Fuzzy Trust-Based Filtering*[7] - Fuzzy classification of packet delivery

Single-Metric TMFs II

- 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

Multi-Metric TMF

Multi-metric Trust For MANETS (MTFM)[1]

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

Multi-Metric TMF

Multi-metric Trust For MANETS (MTFM)[1]

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

Operates favourably in 802.11 against OTMF and Hermes, accurately detecting, identifying, & characterising misbehaviours.[1]

Multi-Metric TMF - Grey Grading

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

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

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

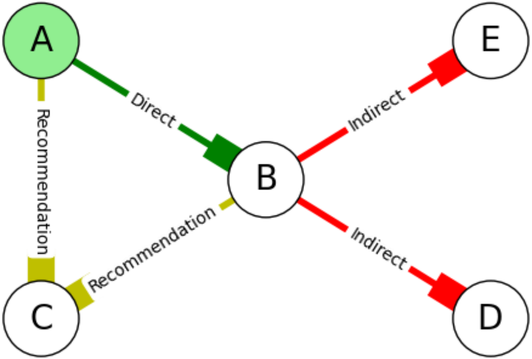
$$T_k^t = (1 + (\phi_k^t)^2/(\theta_k^t)^2)^{-1} \tag{4}$$

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

Multi-Metric TMF - Topological Relationships

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

$$T^{MTFM}_{i,j}$$



1 ▸ Details

Outline

Communications Channel Considerations

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

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

Attenuation in the Marine Acoustic Channel

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

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

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient;[11]

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

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

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

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient;[11]

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

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

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

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

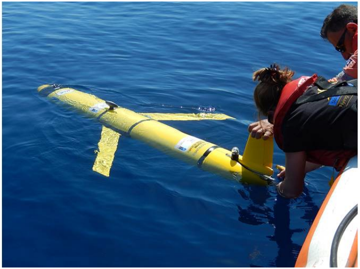


Fig. 1: REMUS 100 AUV as deployed at NATO CMRE La Spezia

Operational Considerations: Collaborative AUV Survey

Context:

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

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

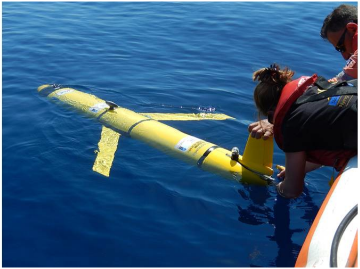


Fig. 1: REMUS 100 AUV as deployed at NATO CMRE La Spezia

Outline

Misbehaviour Specification

- Two misbehaviours investigated:
  - *Malicious Power Control*(MPC) - attacker aims to make a node appear selfish by increasing power to all nodes except to/from it
  - *Selfish Target Selection*(STS) - node preferentially communicates with nodes close to it, to conserve its own power.
- Neither misbehaviour directly affects PLR, while impacting network fairness,
- Default Behaviour: random walk with "Fair" communications
- Three Scenarios:
  - All nodes are Fair
  - One node is Malicious (MPC)
  - One node is Selfish (STS)

Scaling Considerations

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

Scaling 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 optimising for delay/throughput ▸ Details
- Six per-link communications metrics

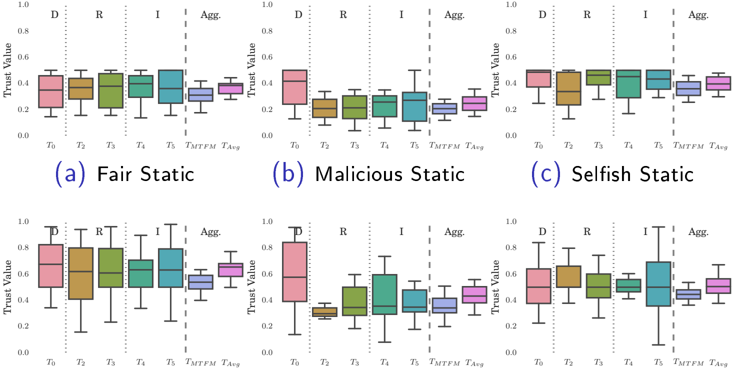
Scaling Considerations

- 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 optimising for delay/throughput ▸ Details
- Six per-link communications metrics

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

Outline

Multi-Metric Operation I



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

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

Fig. 2: Observations of n_1 $(T_{1,X})$, showing Direct, Recommender and Indirect relationships and T_{MTFM} and T_{AVG}Y ▸ Closeup

Multi-Metric Operation II

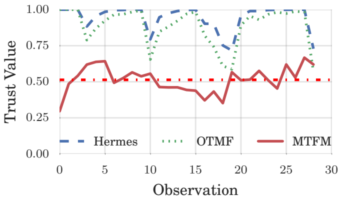
Key Observations:

- Mobility greatly increases variation in observed trust
- T_{MTFM} remains more stable in both mobility cases when compared to either single-node assessments or T_{Avg}
- Raw T_{MTFM} isn't perfect; results demonstrate huge variability in Direct assessment ($T_{1,0}$) that isn't reflected in T_{MTFM}.
- Larger variability in "Fair" case compared to MPC/STS

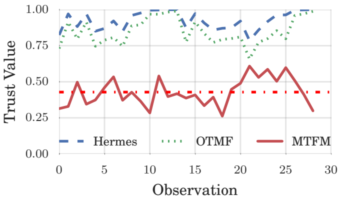
Considering the mobility results and stated context, we continue with mobile-only scenarios.

Outline

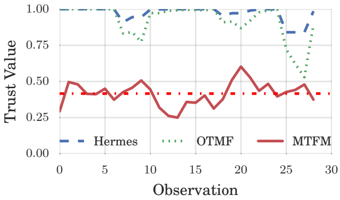
Blind Comparison of Single/Multi-metric TMFs



(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

Key Observations:

- Everybody Sucks

Blind Comparison of Single/Multi-metric TMFs

Key Observations:

- Everybody Sucks
- Neither OTMF, Hermes or Blind MTFM are effective
- MTFM's Comparison means in the fair case, ≈ 0.5 is expected
- In OTMF/Hermes, $T \approx 1$ is expected

Blind Comparison of Single/Multi-metric TMFs

Key Observations:

- Everybody Sucks
- Neither OTMF, Hermes or Blind MTFM are effective
- MTFM's Comparison means in the fair case, ≈ 0.5 is expected
- In OTMF/Hermes, $T \approx 1$ is expected
- MTFM indicates $\approx 10\%$ selectivity between Fair and Either Misbehaviour

Blind Comparison of Single/Multi-metric TMFs

Key Observations:

- Everybody Sucks
- Neither OTMF, Hermes or Blind MTFM are effective
- MTFM's Comparison means in the fair case, ≈ 0.5 is expected
- In OTMF/Hermes, $T \approx 1$ is expected
- MTFM indicates $\approx 10\%$ selectivity between Fair and Either Misbehaviour

BUT!

Blind Comparison of Single/Multi-metric TMFs

Key Observations:

- Everybody Sucks
- Neither OTMF, Hermes or Blind MTFM are effective
- MTFM's Comparison means in the fair case, ≈ 0.5 is expected
- In OTMF/Hermes, $T \approx 1$ is expected
- MTFM indicates $\approx 10\%$ selectivity between Fair and Either Misbehaviour

BUT! MTFM allows exploration of the metric space.

Outline

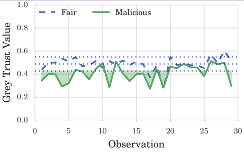
Metric Weighting

From (3), metric emphasise can be adjusted

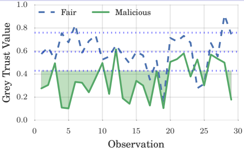
$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t\right] \tag{7}$$

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

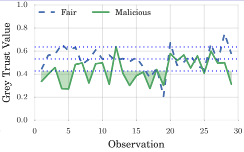
Malicious Power Control - Weighted Emphasis



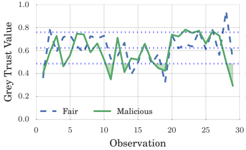
(a) Delay Emphasised



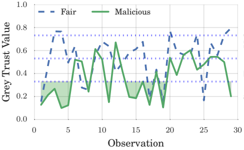
(b) PLR Emphasised



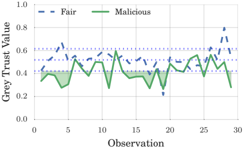
(c) RX Power Emphasised



(d) TX Power Emphasised



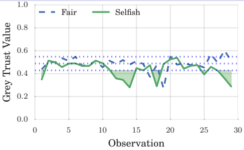
(e) RX Throughput Emphasised



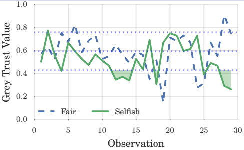
(f) TX Throughput Emphasised

Fig. 3: $T_{1,MTFM}$ in the All Mobile case for the Malicious Power Control behaviour, including dashed $\pm\sigma$ envelope about the fair scenario ▸ Closeup

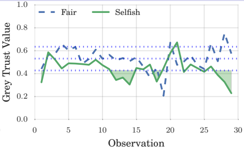
Selfish Target Selection - Weighted Emphasis



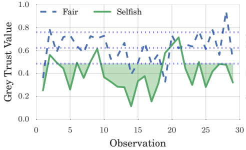
(a) Delay Emphasised



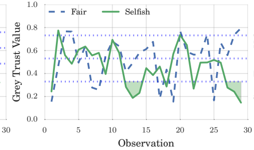
(b) PLR Emphasised



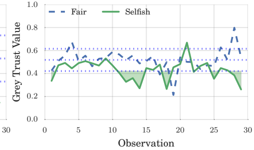
(c) RX Power Emphasised



(d) TX Power Emphasised



(e) RX Throughput Emphasised



(f) TX Throughput Emphasised

Fig. 4: $T_{1,MTFM}$ 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 most
  - Particularly PLR
  - Less so in Delay, P_{RX} and T_{TX}
- In STS case:
  - Less overall impact
  - Stronger impact of P_{TX}

Outline

Regression of Metric Significance

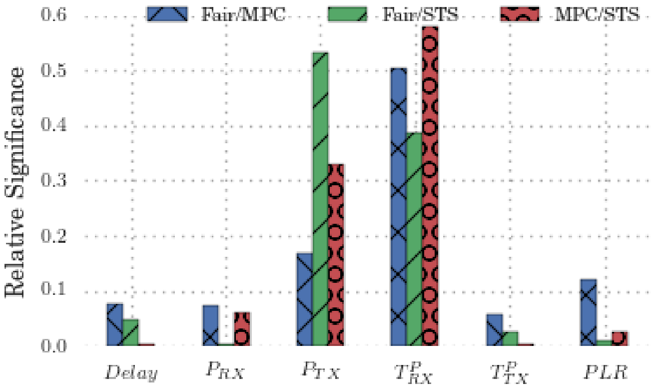
Aim: Establish which metrics are important in discriminating behaviours

Regression of Metric Significance

Aim: Establish which metrics are important in discriminating behaviours

- Distributed Random Forest Regression[14]
- 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

Metric Significance



Metric Correlation Combs

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

Key Observations

- PLR not necessarily the most important metric in discriminating behaviours

Key Observations

- PLR not necessarily the most important metric in discriminating behaviours
- Combination of Significance and Correlations demonstrate selectivity opportunity

Key Observations

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

Key Observations

- PLR not necessarily the most important metric in discriminating behaviours
- 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

Key Observations

- PLR not necessarily the most important metric in discriminating behaviours
- 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

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

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
  - Perform / Initiate practical trials in collaborations with NATO CMRE

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. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011* (2011), pp. 142–149. DOI: 10.1109/TrustCom.2011.21. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120813.

References II

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

Charikleia Zouridaki et al. "A quantitative trust establishment framework for reliable data packet delivery in MANETs". In: *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks* (2005), pp. 1–10. ISSN: 0926227X. DOI: 10.1145/1102219.1102222.

References III

- Jie Li et al. "Future Trust Management Framework for Mobile Ad Hoc Networks". In: *IEEE Communications Magazine* 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.

References IV

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

Junhai Luo et al. "Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks". In: *2008 33rd IEEE Conference on Local Computer Networks (LCN)* (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. ISBN: 0070660867.

Jim Partan, Jim Kurose, and Brian Neil Levine. “A survey of practical issues in underwater networks”. In: *Proceedings of the 1st ACM international workshop on Underwater 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.

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.

References VI

Andrej Stefanov and Milica Stojanovic. "Design and performance analysis of underwater acoustic networks". In: *IEEE Journal on Selected Areas in Communications* 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.

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.

References VII

L Breiman. “Random forests”. In: *Machine learning* (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.

Thank You

Grey Trust Equs I

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

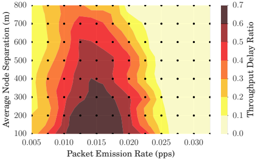
Where $T_{i,n}$ is the subjective trust assessment of n_i by n_n, and $f_s = [f_1, f_2, f_3]$ given as...

Grey Trust Equs II

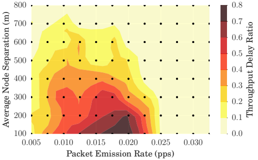
$$
\begin{aligned}
f_1(x) &= -x + 1 \\
f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\
f_3(x) &= x
\end{aligned}
\tag{10}
$$

Back

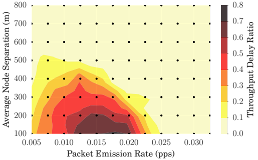
Comms Scaling Graphs I



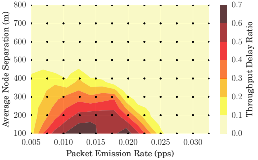
(a) All Nodes Static



(b) n_1 Random Walk



(c) All nodes but n_1 Random Walk



(d) All nodes Random Walk

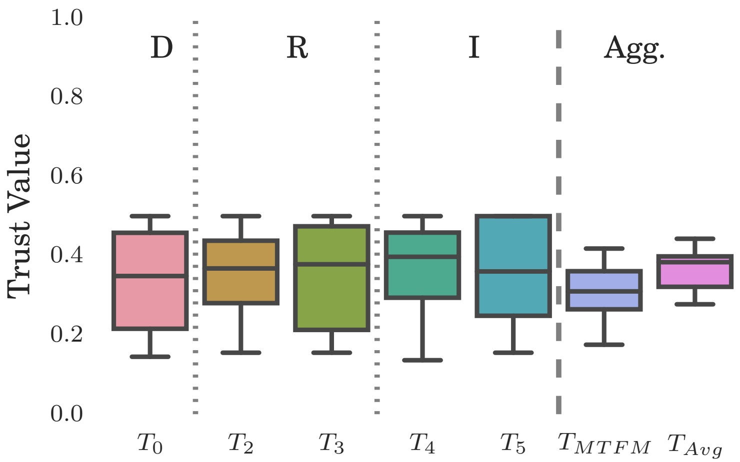
Back

System Model Constraints

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

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

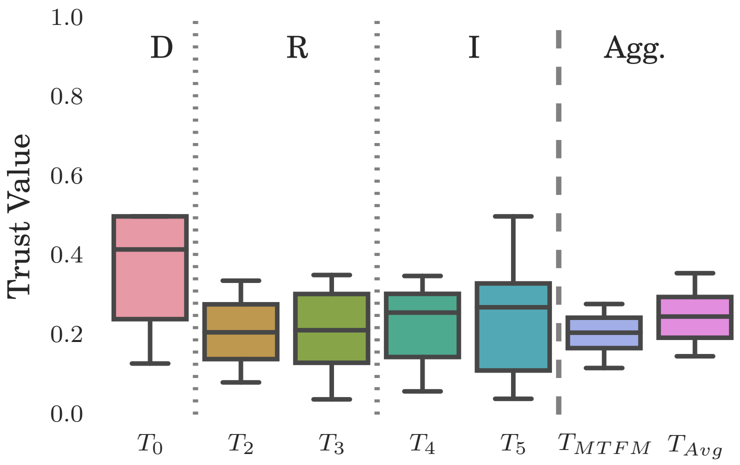
MTFM Operation Detail



(a) Fair Static

Back

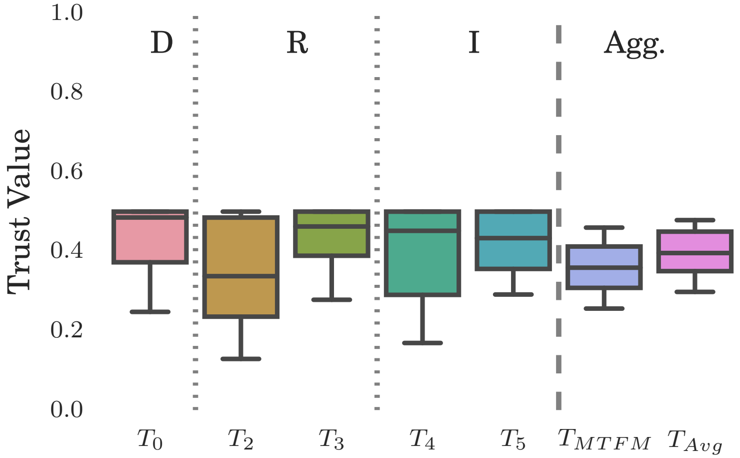
MTFM Operation Detail



(b) Malicious Static

Back

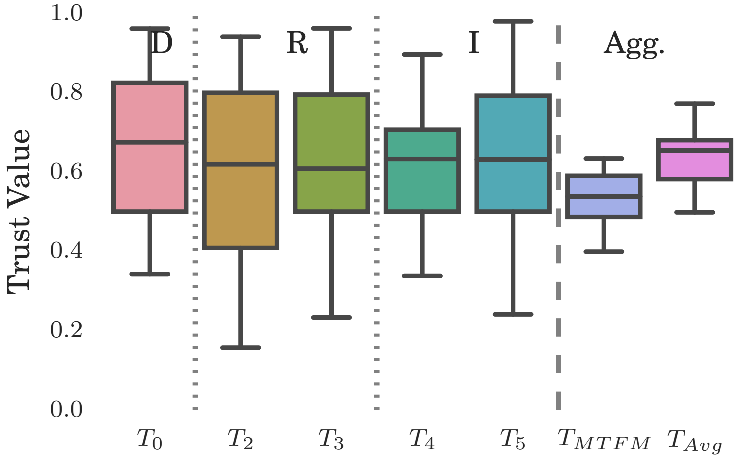
MTFM Operation Detail



(c) Selfish Static

Back

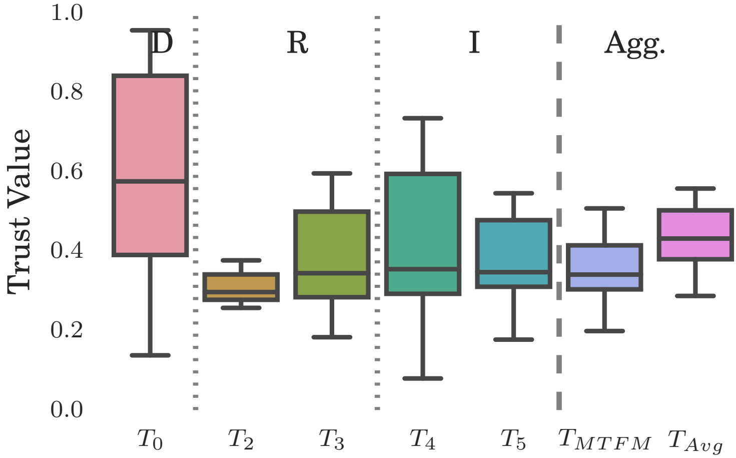
MTFM Operation Detail



(d) Fair Mobile

Back

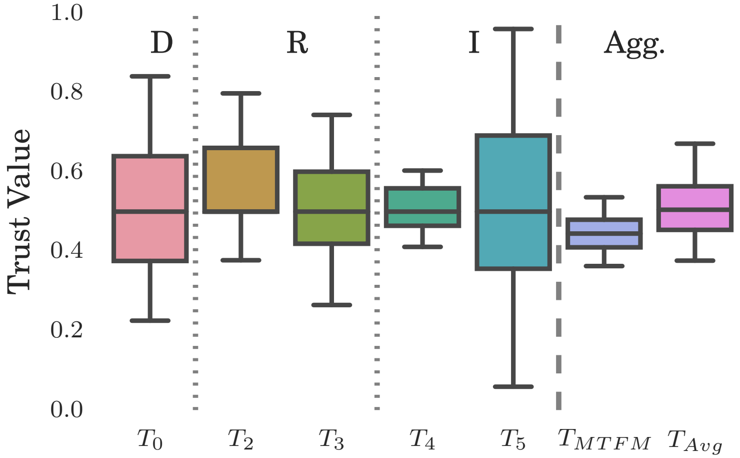
MTFM Operation Detail



(e) Malicious Mobile

Back

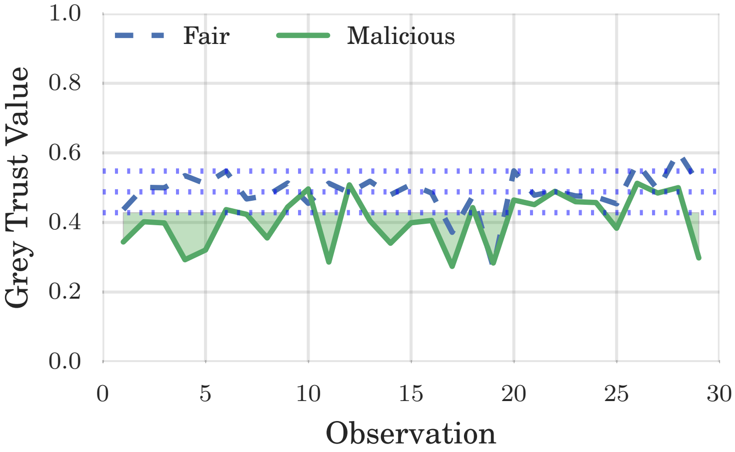
MTFM Operation Detail



(f) Selfish Mobile

Back

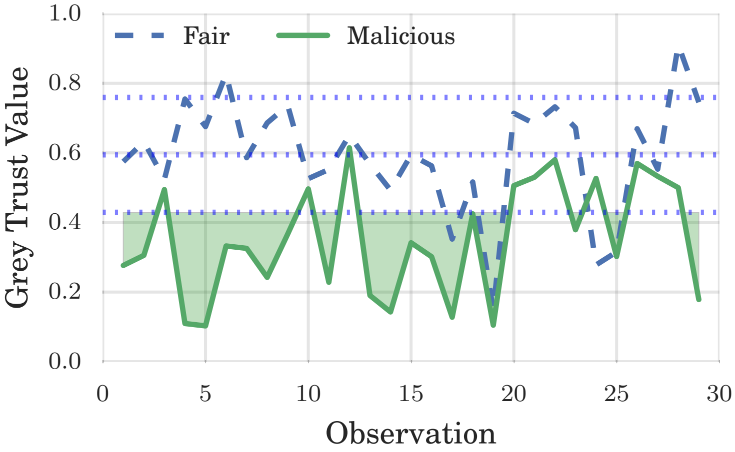
MTFM Malicious Power Control Detail



(a) Delay Emphasised

Back

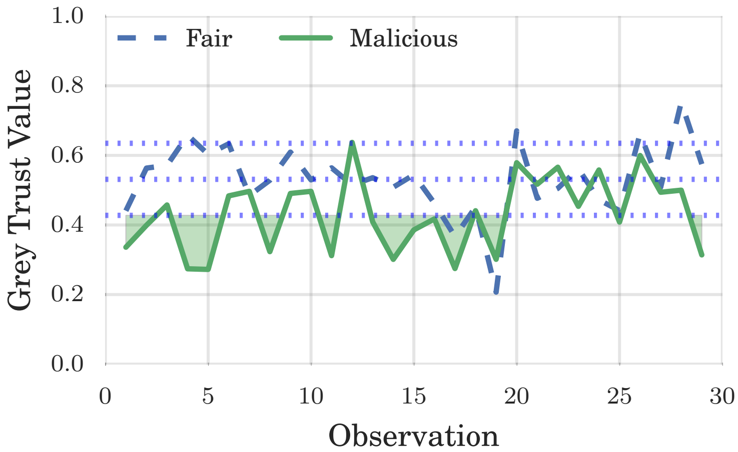
MTFM Malicious Power Control Detail



(b) PLR Emphasised

Back

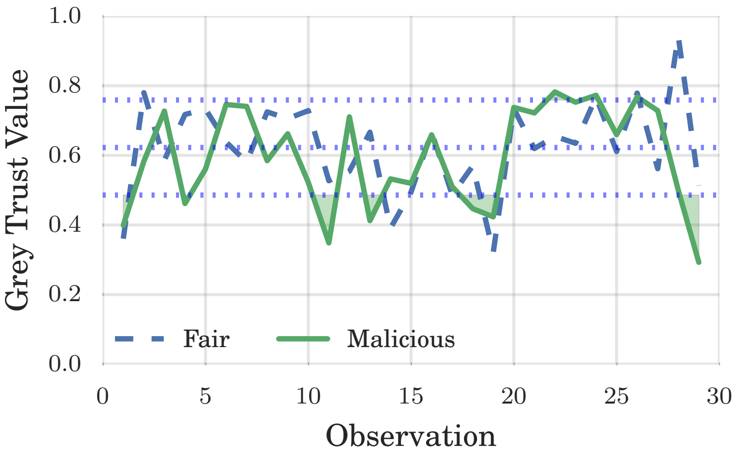
MTFM Malicious Power Control Detail



(c) RX Power Emphasised

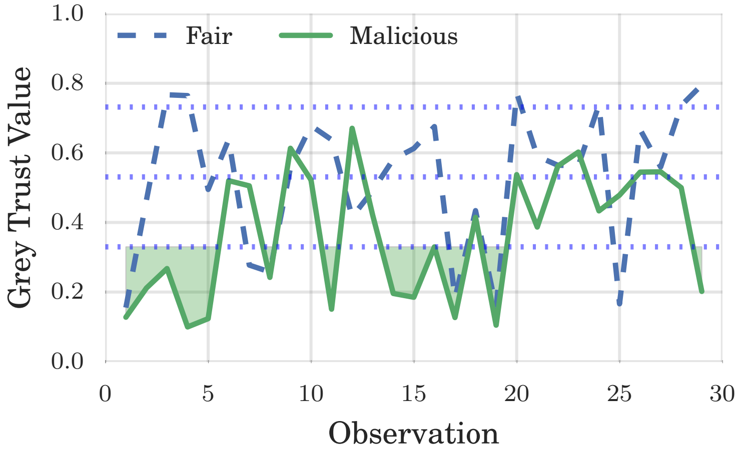
▸ Back

MTFM Malicious Power Control Detail



(d) TX Power Emphasised

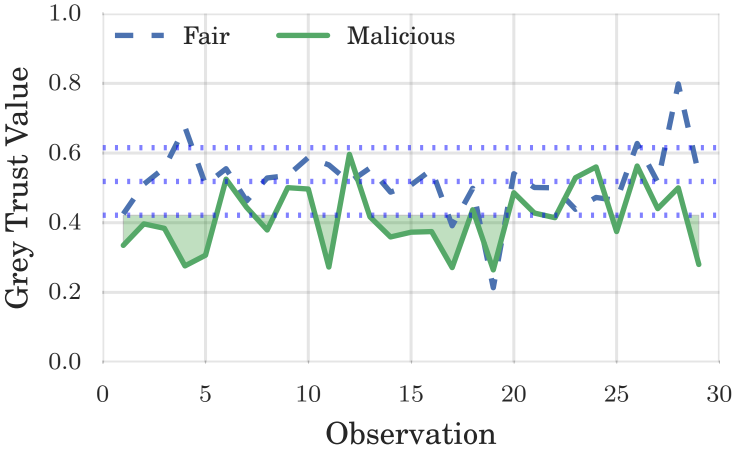
MTFM Malicious Power Control Detail



(e) RX Throughput Emphasised

Back

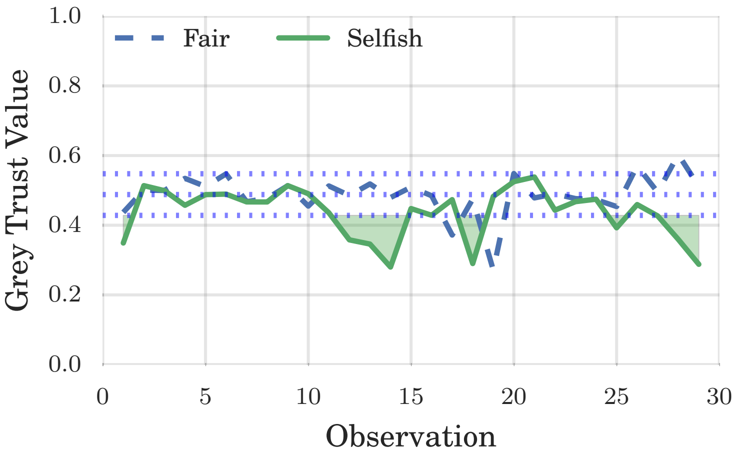
MTFM Malicious Power Control Detail



(f) TX Throughput Emphasised

Back

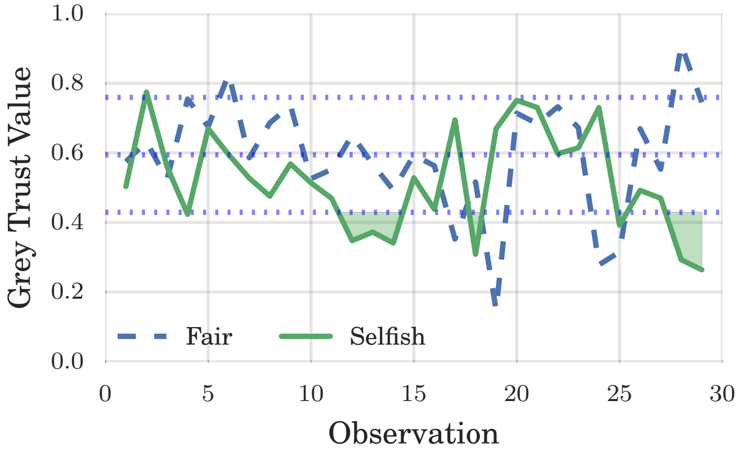
MTFM Selfish Target Selection Detail



(a) Delay Emphasised

▸ Back

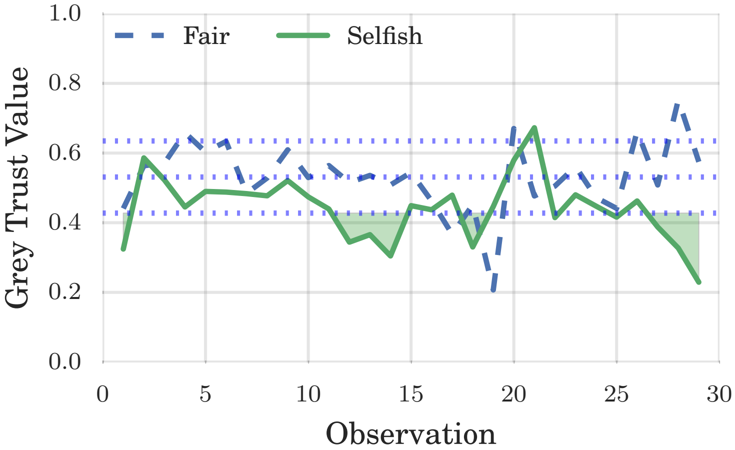
MTFM Selfish Target Selection Detail



(b) PLR Emphasised

Back

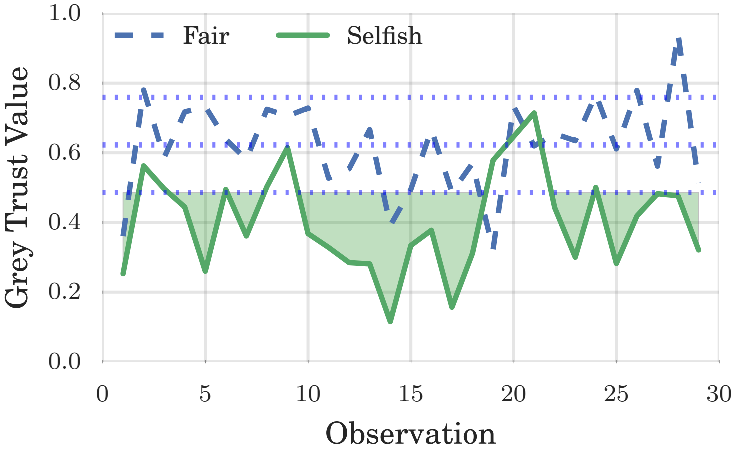
MTFM Selfish Target Selection Detail



(c) RX Power Emphasised

▸ Back

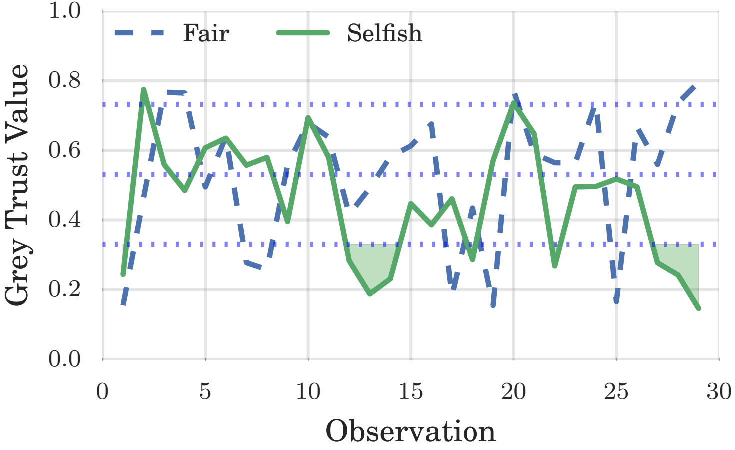
MTFM Selfish Target Selection Detail



(d) TX Power Emphasised

Back

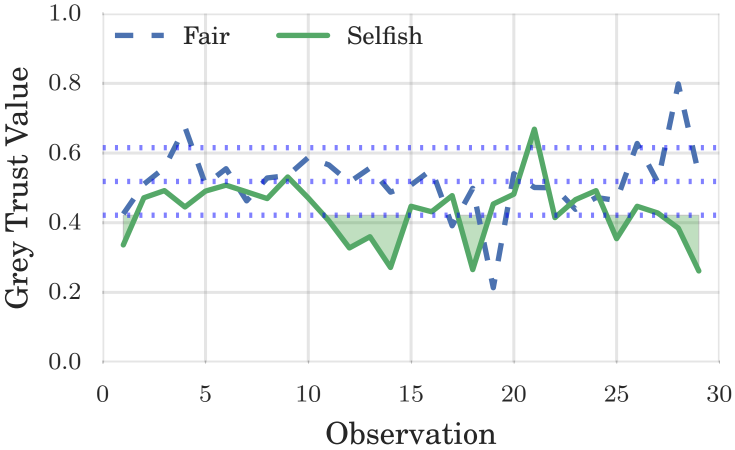
MTFM Selfish Target Selection Detail



(e) RX Throughput Emphasised

Back

MTFM Selfish Target Selection Detail



(f) TX Throughput Emphasised

Back