# 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)

# Summary





- Methods developed for establishing Communications Trust in the MANET space increasingly applied to other arenas such as the underwater realm.
- These Trust Management Frameworks (TMFs) must be reassessed with respect to the sparse, noisy and contested marine communications environment.
- Most MANET TMFs 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 success observation

# Outline

# 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] - Probablistic 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 eg Topology

# Single-Metric TMFs II



- Single Metric TMFs present opportunities for malicious actors to undermine the operation of a network if their attack does not directly impact packet delivery.
- Not an issue in networks where Comms. is the primary operating concern, but is significant in resource constrained environments (eg 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

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

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

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

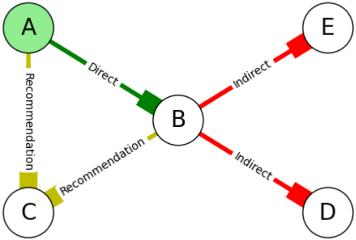
$$T^t_k = (1 + (\phi^t_k)^2 / (\theta^t_k)^2)^{-1} \tag{4}$$

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 misbehavor.

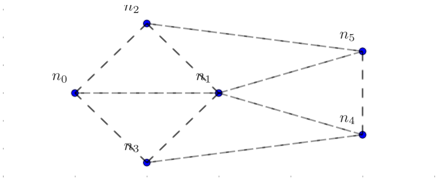



Fig. 1: Initial Node Layouts in [1]

# Outline

# Communications Channel Considerations I

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

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

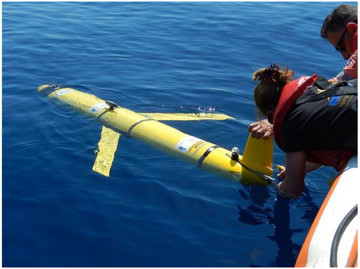


Fig. 2: REMUS 100 AUV as deployed at NATO CMRE La Spezia

# 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

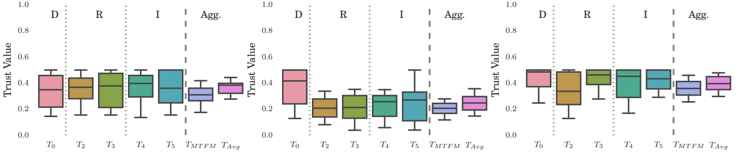
- Motivation
  - Related Work
  - Challenges to Trust in Underwater Networks
- Our Contribution
  - Experimental Context
  - Main Results
  - Current Work

# Principal Aims

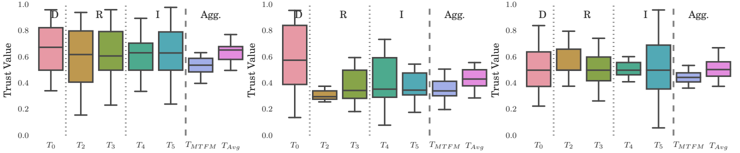
- Operation of MTFM in the Marine Environment
- 

# Multi-Metric Operation I






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




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

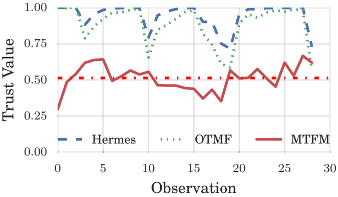
Fig. 3: Observations of $n_1$ ($T_{1,X}$), showing Direct, Recommender and Indirect relationships and $T_{MTFM}$ and $T_{AVG}$ ▸ Closeup

# Multi-Metric Operation II

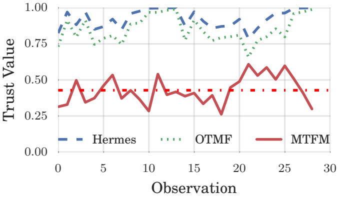
Key Observations:

- Mobility greatly increases variation in instantenously 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 4e 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

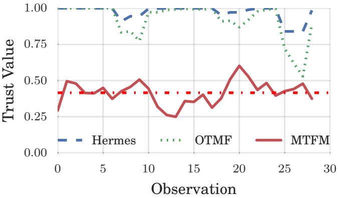
# Blind Comparison of Single/Multi-metric TMFs I




(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:

- 

# Metric Significance Assessment

# Outline

# Current Work and Paths to Proof/Implementation

# Make Titles Informative.

# Summary





- The first main message of your talk in one or two lines.
- The second main message of your talk in one or two lines.
- Perhaps a third message, but not more than that.

- Outlook
  - Something you haven't solved.
  - Something else you haven't solved.

# 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.

# References III


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.

The End

# Grey Trust Equs I

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

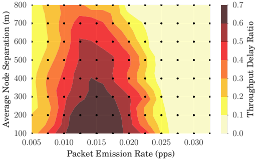
Where $T_{i,n}$ is the subjective trust assessment of $n_i$ by $n_n$, and $f_s = [f_1, f_2, f_3]$ given as...

# Grey Trust Equs II

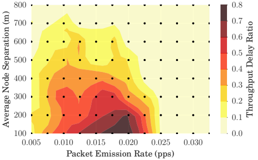
$$
\begin{aligned}
f_1(x) &= -x + 1 \\
f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\
f_3(x) &= x
\end{aligned} \tag{8}
$$

# Comms Scaling Graphs I

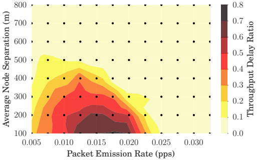




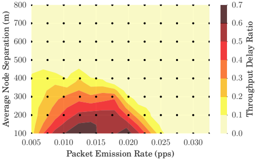

(d) All Nodes Static




(e) $n_1$ Random Walk




(f) All nodes but $n_1$ Random Walk




(g) All nodes Random Walk

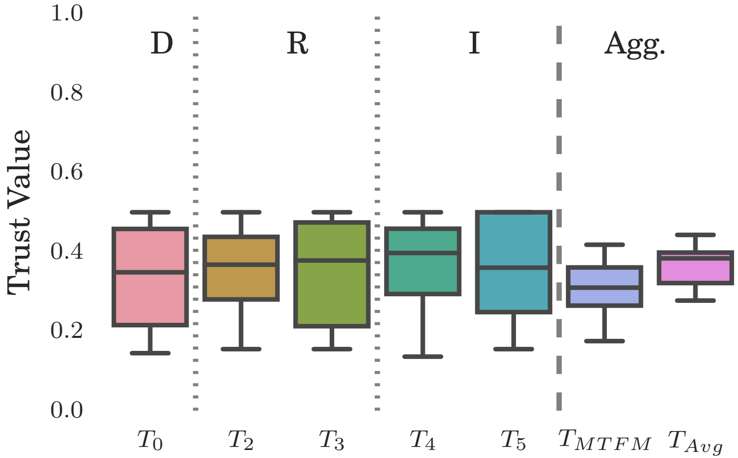
# System Model Constraints



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

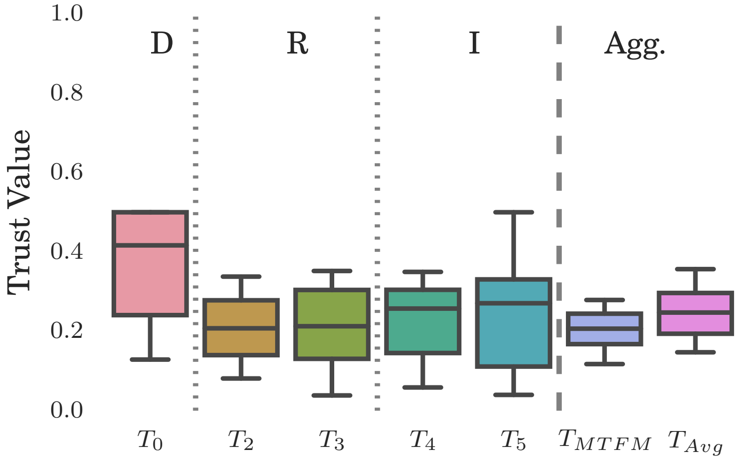
| Parameter | Unit | Terrestrial | Marine |
|---|---|---|---|
| Simulated Duration | $s$ | 300 | 18000 |
| Trust Sampling Period | $s$ | 1 | 600 |
| Simulated Area | $km^2$ | 0.7 | 0.7-4 |
| Transmission Range | $km$ | 0.25 | 1.5 |
| Physical Layer | | RF(802.11) | Acoustic |
| Propagation Speed | $m/s$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

# MTFM Operation Detail



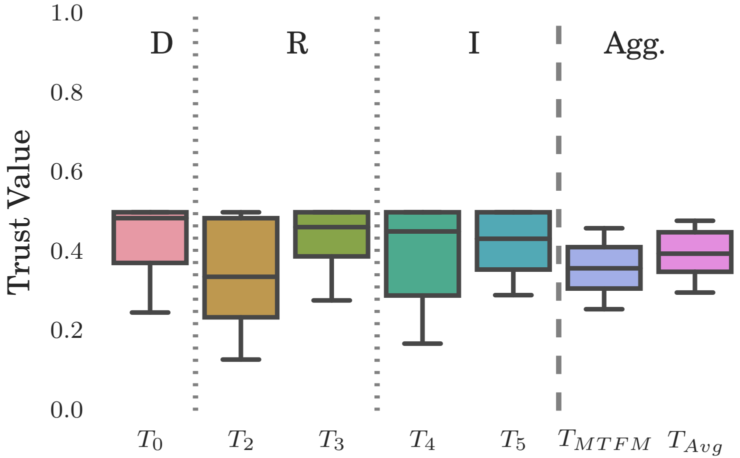

(a) Fair Static

# MTFM Operation Detail




(b) Malicious Static

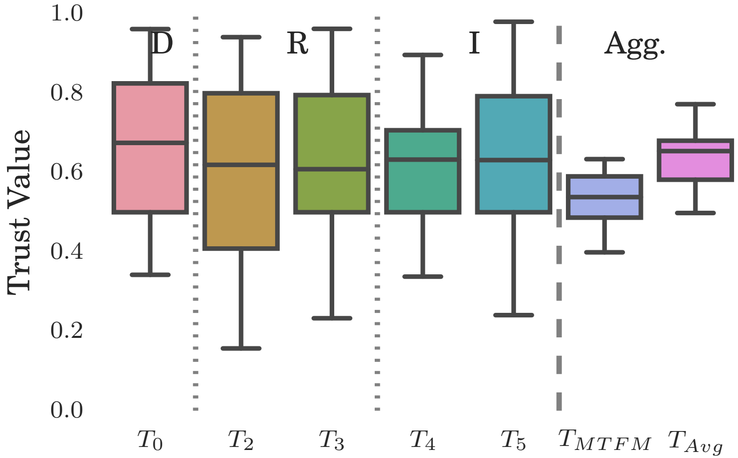
# MTFM Operation Detail




(c) Selfish Static

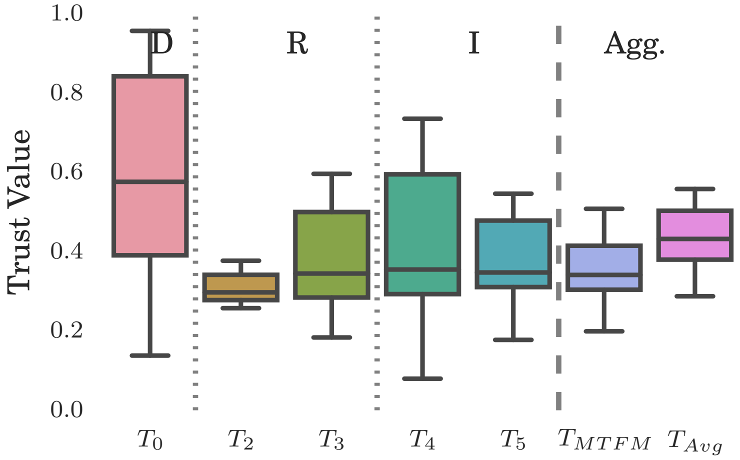
# MTFM Operation Detail






(d) Fair Mobile

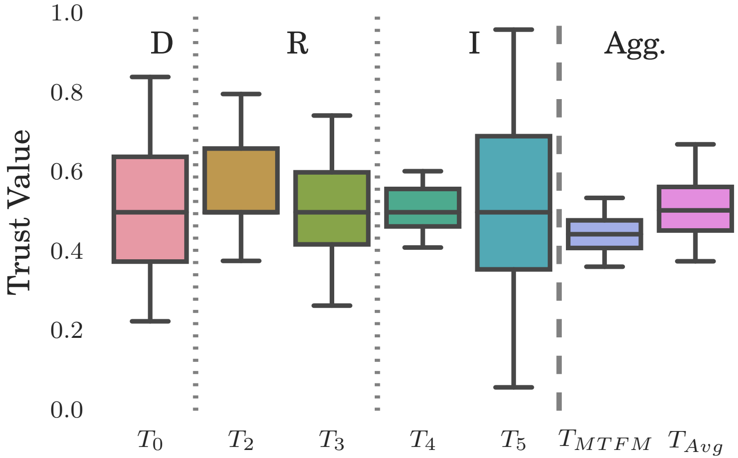
# MTFM Operation Detail




(e) Malicious Mobile

# MTFM Operation Detail






(f) Selfish Mobile