

An Investigation into Trust and Reputation Frameworks for Autonomous Underwater Vehicles

Author: Andrew Bolster

Supervisors: Prof. Alan Marshall, Prof. Simon Maskell (UoL)
Prof. Jean-Guy Fontaine (UPMC)

University of Liverpool

Thursday 6th October 2016

- 1 Structure
- 2 Contributions, Errata & State of the Field
- 3 Chapter Summaries

Structure of this presentation

Structure

- Statement of Research Purpose
- Summary of Contributions
- Errata
- Discussion of new research that has entered the field since submission
- Chapter Summaries
- Open for Discussion

Summary of Contributions

Primary

- Trust in UANs
- Trust assessment based on Physical Behaviours
- Multi-domain Trust assessment

Secondary

- Automatic, behaviour based weighting of MTFM
- Agent based UAN Simulation system
- Synthetic Domains based on metrics across multiple domains
- Review of Trust in the marine defence context

Publications

- Analytical Metric Weight Generation for Multi-Domain Trust in Autonomous Underwater MANETs. IEEE UComms 2016
- Single and Multi-metric Trust Management Frameworks for Use in Underwater Autonomous Networks. IEEE TrustCom 2015
- Analysis of Trust Interfaces in Autonomous and Semi-Autonomous Collaborative MHPC Operations, The Technical Cooperation Program, Portsmouth, UK 2014.
- A Multi-Vector Trust Framework for Autonomous Systems, AAAI 2014.

Erratta

- Many small typographic issues corrected
- Missing Citation in 3.1.1,5-7^a
- Out-of-order paragraphs in 4.2.5 (Top should be bottom)

^aR J Urick (1983). *Principles of underwater sound*. NewYork.423pages. ISBN: 0070660867.

Trust

- Interesting general move towards decentralised trust^a
- Ditto cohort based relative trust assessment^b
- Increasing use of ML techniques to assess contextual trust dynamically^c
- Human Factors emerging as a increasingly vital area of research^d
- Novel/Updated techniques for generalised TMF assessment are emerging^e

^aKorzun et al., 2015.

^bSingh and Sidhu, 2016.

^cRishwaraj, Ponnambalam, and Loo, 2017.

^dSaeidi, 2009; Matthews et al., 2016; Lahijanian and Kwiatkowska, 2016.

^eJaniszewski, 2016.

Acomms

- Assumptions of Gaussian noise naive for real applications^a
- The Beaufort Sea has fundamentally changed it's characteristics in 20 years and highlights fundamental flaws in channel modelling assumptions^b
- Higher-Stack level functionality problems remain open(i.e. MAC+Route+ID+Interop)^c
- Assumptions on increasing accuracy and timeliness of passive localisation proving accurate^d

^aMahmood and Chitre, 2016; Deane and Preisig, 2016.

^bSchmidt and Schneider, 2016.

^cDiamant, Francescon, and Zorzi, 2016; Petroccia, 2016; Petroccia, Alves, and Zappa, 2016; Anjangi and Chitre, 2016.

^dVio, Cristi, and Smith, 2016; Ferreira et al., 2016; Das and Thampi, 2016.

Focus On

- Trust
- Autonomy
- Decentralised networks
- Harsh Environments

Stated deficiencies in

- Single Metric Trust
- Threats from Capable actors
- Systemic Trust
- Lack of modelling of Trust in Harsh environments

Chapter 2: MANETs and Trust

Focus On

- Network/Graph concepts
- Routing
- Trust Perspectives and Models
- Trust Relationships
- Multi-Party Trust
- Trusted Threats
- Autonomy and Design constraints of Autonomous Systems
- Current Trust Management Frameworks

Key Outcomes

- Definition of Trust
- Levels & Constraints of Autonomy
- Lack Specification and Validation for Autonomous Systems
- Threats to Trust
- Threats to MANETs
- Need for Trust in Autonomous Systems

Chapter 3: Maritime Communications and Operations

Focus On

- Marine Acoustics
- AComms Modelling
- AUV Operations
- Need for Trust in AUV AComms

Key Outcomes

- Channel Emulation Models
- Selection of characteristic constraints
- Threat Surface
- Operational / Kinematic constraints and Scenario selection

Chapter 4: Assessment of TMF Performance in Marine Environments

Focus On

- Comparative factors between UAN/WLAN
- Relevant Metric Selection re AComms
- Comparison of Single & Multi Metric TMFs in UAN
- MTFM weight variation assessment and regression

Key Findings

- Modelled optimal performance range @ $\approx 0.015\text{-}0.025\text{pps}/100\text{-}300\text{m}$ node separations [▶ Details](#)
- MTFM outperforms single metric TMFs for selected misbehaviours [▶ Details](#)
- MTFM vector weighting further improves performance and tolerance [▶ Details](#)
- Long collection times due to sparsity can impact trust assessment relevance

Chapter 5: Use of Physical Behaviours for Trust Assessment

Focus On

- Physical Misbehaviours and Metrics
- “Failure” vs “Selfish” vs “Malice”
- AUV Kinematics
- Metric variability in collaborative collision avoidance (flocking)
- Metric based classifier

Key Findings

- First physical misbehaviour detection system in UAN
- Demonstrated that different misbehaviours impact different physical metrics differently [► Details 1](#) [► Details 2](#)
- Highly accurate, manually configured, blind behaviour classifier ($\approx 0\%$ FP, $\approx 90\%$ TP)

Chapter 6: Multi-Domain Trust Assessment in Collaborative Marine MANETs

Focus On

- Combination of comms. & phys. metrics
- Random Forest based metric significance correlation to build H weighting vector for MTFM
- Domain specific behaviour effects across domain space
- Relative vector weight measurement across cohort ($\Delta T, \Delta T^-$)
- Generation and Appraisal of alternate/targeted “domains”

Key Findings

- Misbehaviours impact across domains (not obvious) [▶ Details](#)
- Inherent redundancy (eg $INDD/P_{RX}$) allows differential behaviours to be detected [▶ Details](#)
- Application level selfishness (STS) very difficult to automatically
- Extended Ch4 behaviour based optimisation of MTFM to dynamically select most significant metrics




Summary of Contributions to the Field

Σ


- UWA Multi Metric/Domain Trust
- UWA Trust is **Hard** & it's mostly the channels' fault
- Discrimination of non-comms misbehaviours/failures **even just using comms metrics**
- Methodology for exploring / training / metric relevance
- Single-Metric Trust is **unstable** in such an environments
- Multi-Metric Trust works & can **discriminate behaviours**
- **Not all metrics** are equally useful
- Simple classifiers **can** be very good in **some** behaviours (MPC)
- - can be **not so good** for others (STS)









- Smarter Detection Classifier
- Cooperative / Periodic / Variable attack profiles
- Further assessment of impact and tolerance of misbehaviours in the network
- Commonality of detection filters across Multiple-base scenarios
- **Real** experiments and Cross validation implementations
- Heterogenous Node capabilities / Mixed-mission characteristics
- Extension to logical routing domain
- Application of mixed-domain trust assessment to non-physical systems
- Reflective Trust (i.e. systems trust of the operator)

-  Urick, R J (1983). *Principles of underwater sound*. New York. 423 pages. ISBN: 0070660867.
-  Korzun, Dmitry G. et al. (2015). "Internet of Things, Smart Spaces, and Next Generation Networks and Systems". In: *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)* 9247, pp. 56–67. ISSN: 16113349. DOI: 10.1007/978-3-319-23126-6. URL: <http://www.scopus.com/inward/record.url?eid=2-s2.0-84948975701%7B%5C%7DpartnerID=tZ0tx3y1>.
-  Singh, Sarbjeet and Jagpreet Sidhu (2016). "Compliance-based Multi-dimensional Trust Evaluation System for determining trustworthiness of Cloud Service Providers". In: *Futur. Gener. Comput. Syst.* 67, pp. 109–132. ISSN: 0167739X. DOI: 10.1016/j.future.2016.07.013. URL: <http://dx.doi.org/10.1016/j.future.2016.07.013>.






References II




-  Rishwaraj, G, S G Ponnambalam, and Chu Kiong Loo (2017). "Trust Evaluation in a Multi-robotics System Through Direct Learning". In: *9th Int. Conf. Robot. Vision, Signal Process. Power Appl. Empower. Res. Innov.* Ed. by Haidi Ibrahim et al. Singapore: Springer Singapore, pp. 407–417. ISBN: 978-981-10-1721-6. DOI: 10.1007/978-981-10-1721-6_44. URL: http://dx.doi.org/10.1007/978-981-10-1721-6_7B%5C_%7D44.
-  Saeidi, Hamed (2009). "Trust-Based Control of (Semi)Autonomous Mobile Robotic Systems". In:
-  Matthews, G et al. (2016). "Resilient Autonomous Systems : Challenges and Solutions". In: pp. 208–213.
-  Lahijanian, Morteza and Marta Kwiatkowska (2016). "Social Trust : a Major Challenge for the Future of Autonomous Systems". In: October.

References III

-  Janiszewski, Marek B. (2016). "Methods for reliability evaluation of trust and reputation systems". In: 10031, 100314B. DOI: 10.1117/12.2248791. URL: <http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2248791>.
-  Mahmood, Ahmed and Mandar Chitre (2016). "Uncoded Acoustic Communication in Shallow Waters with Bursty Impulsive Noise". In: *Underw. Commun. Netw.*
-  Deane, Grant and J. Preisig (2016). "Very High Frequency Noise Sources in the Littoral Zone". In: *Underw. Commun. Netw.*
-  Schmidt, Henrik and Toby Schneider (2016). "Acoustic Communication and Navigation in the New Arctic - A Model Case for Environmental Adaptation". In: *Underw. Commun. Netw.*
-  Diamant, Roee, Roberto Francescon, and Michele Zorzi (2016). "Efficient Link Discovery for Underwater Networks". In: *Underw. Commun. Netw.*
-  Petroccia, Roberto (2016). "A Distributed ID Assignment and Topology Discovery Protocol for Underwater Acoustic Networks". In: *Underw. Commun. Netw.*

References IV

-  Petroccia, Roberto, J. Alves, and G. Zappa (2016). "Fostering the Use of JANUS in Operationally-Relevant Underwater Applications". In: *Underw. Commun. Netw.*
-  Anjangi, Prasad and Mandar Chitre (2016). "Unslotted Transmission Schedules for Practical Underwater Acoustic Multihop Grid Networks with Large Propagation Delays". In: *Underw. Commun. Netw.*
-  Vio, Renato, Roberto Cristi, and Kevin Smith (2016). "Near real-time improved UUV positioning through channel estimation". In: *Underw. Commun. Netw.*
-  Ferreira, Beatriz et al. (2016). "Collaborative Localization of Vehicle Formations Based on Ranges and Bearings". In: *Underw. Commun. Netw.*
-  Das, Anjana P and Sabu M Thampi (2016). "Fault-resilient localization for underwater sensor networks". In: *Ad Hoc Networks*, pp. 1–11. ISSN: 1570-8705. DOI: [10.1016/j.adhoc.2016.09.003](https://doi.org/10.1016/j.adhoc.2016.09.003). URL: <http://dx.doi.org/10.1016/j.adhoc.2016.09.003>.

-  Mayer, Roger C, James H Davis, and F David Schoorman (1995). "An Integrative Model of Organizational Trust". In: *Acad. Manag. Rev.* 20.3, pp. 709–734. ISSN: 03637425. DOI: 10.2307/258792. URL: <http://www.jstor.org/stable/258792>.
-  Rotter, Julian B (1967). "A new scale for the measurement of interpersonal trust¹". In: *J. Pers.* 35.4, pp. 651–665. ISSN: 1467-6494. DOI: 10.1111/j.1467-6494.1967.tb01454.x. URL: <http://dx.doi.org/10.1111/j.1467-6494.1967.tb01454.x>.
-  Liu, K. J. Ray and Beibei Wang (2010). *Cognitive Radio Networking and Security: A Game-Theoretic View*. P. 618. ISBN: 9780521762311. DOI: 10.1017/CB09780511778773. URL: http://www.amazon.com/Cognitive-Radio-Networking-Security-Game-Theoretic/dp/0521762316/ref=sr%7B%5C_%7D1%7B%5C_%7D10?s=books%7B%5C%7Die=UTF8%7B%5C%7Dqid=1413413370%7B%5C%7Ds=1-10%7B%5C%7Dkeywords=cognitive+radio%7B%5C%7Dreader%7B%5C_%7D0521762316.

References VI



Partan, Jim, Jim Kurose, and Brian Neil Levine (2006). "A survey of practical issues in underwater networks". In: *Proc. 1st ACM Int. Work. Underw. networks WUWNet 06* 11.4, p. 17. ISSN: 15591662. DOI: 10.1145/1161039.1161045. URL: <http://portal.acm.org/citation.cfm?doid=1161039.1161045>.



Stojanovic, Milica (2007). *On the relationship between capacity and distance in an underwater acoustic communication channel*. DOI: 10.1145/1347364.1347373. URL: <http://www.mit.edu/%7B~%7Dmillitsa/resources/pdfs/bwdx.pdf>.



Stefanov, Andrej and Milica Stojanovic (2011). "Design and performance analysis of underwater acoustic networks". In: *IEEE J. Sel. Areas Commun.* 29.10, pp. 2012–2021. ISSN: 07338716. DOI: 10.1109/JSAC.2011.111211.

Fig 1.1 Multi-Domain Threat Surface

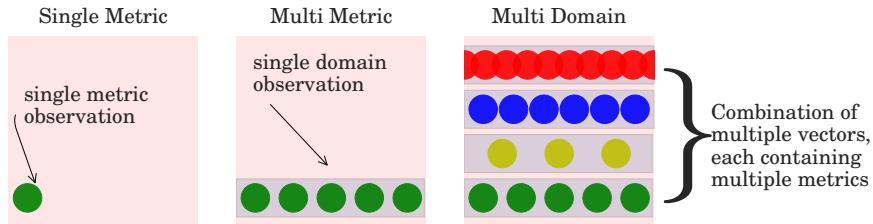


Fig. 1: Multi-Domain Threat Surface

Tab 2.3 Definitions of Trust

Table 1: Selected Definitions of Trust

Definition	Source
Assured reliance on the character, ability, strength, or truth of someone or something.	Merriam-Webster
Firm belief in the reliability, truth, or ability of someone or something	OED
The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party	Mayer, Davis, and Schoorman, (1995)
An expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon	Rotter, (1967)

Fig 2.5 Model of Trust

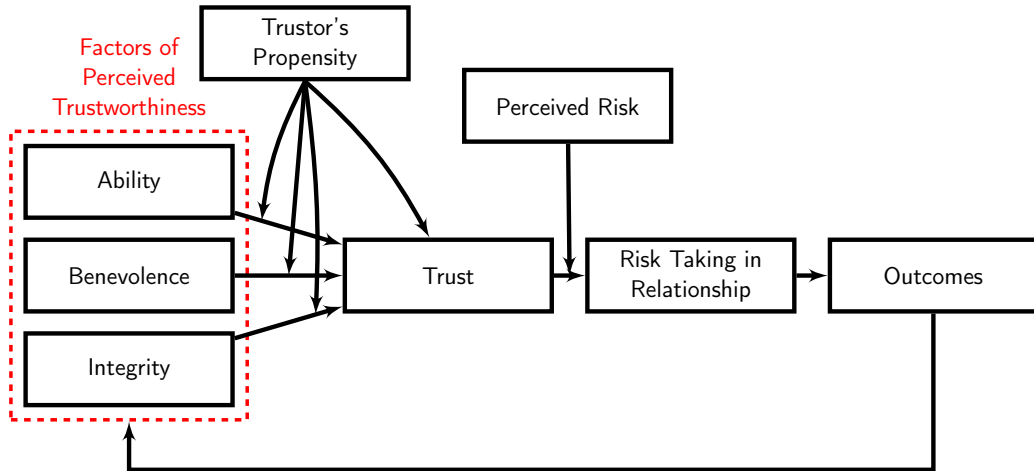


Fig. 2: Model of Trust (from Mayer, Davis, and Schoorman, (1995))

Fig 2.6 Trust Construct Relationships

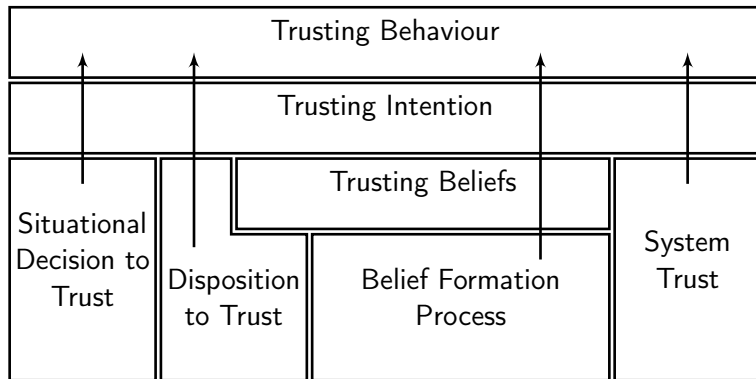


Fig. 3: Trust Construct Relationships (from Liu and Wang, (2010))

Fig 2.10 Trust Topologies

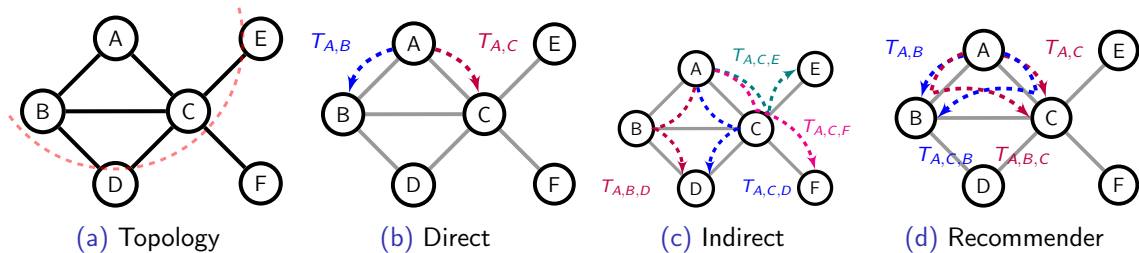
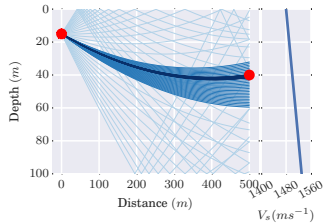
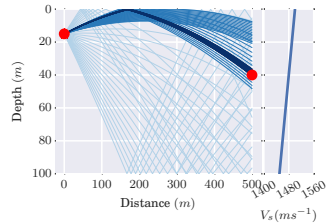


Fig. 4: Trust Topologies; Direct, Indirect, Recommender, etc. from the perspective of Node A

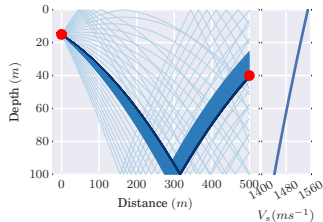
Fig 3.3: Bellhop Model



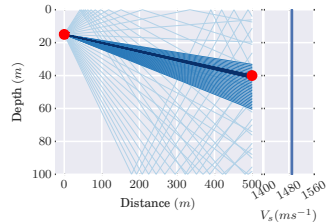
(a) Linear Increasing



(b) Linear Decreasing



(c) Quadratic



(d) Isovelocity

Key Characteristics of the Marine Acoustic Channel Urick, 1983; Partan, Kurose, and Levine, 2006; Stojanovic, 2007; Stefanov and Stojanovic, 2011:

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

$$10 \log A_{\text{aco}}(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \quad (1)$$

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient Stefanov and Stojanovic, 2011;

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

Attenuation in the Marine Acoustic Channel

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

$$10 \log A_{\text{aco}}(d, f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \quad (1)$$

where A_0 is a normalising constant, k is a spreading factor, and $a(f)$ is the absorption coefficient Stefanov and Stojanovic, 2011;

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

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

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

$$\theta_{k,j}^t = \frac{\min_k |a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|}{|a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|} \quad (3)$$

$$\phi_{k,j}^t = \frac{\min_k |a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|}{|a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|} \quad (4)$$

$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^M h_j \theta_{k,j}^t, \sum_{j=0}^M h_j \phi_{k,j}^t \right] \quad (5)$$

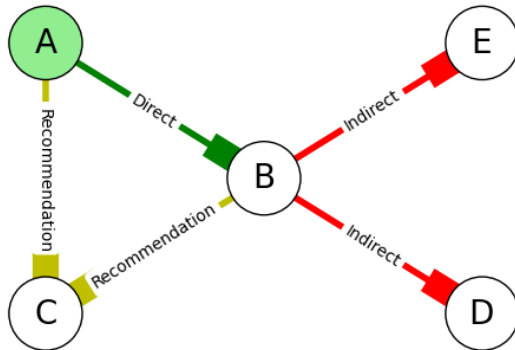
$$\mathcal{T}_k^t = (1 + (\phi_k^t)^2 / (\theta_k^t)^2)^{-1} \quad (6)$$

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 $\{a_{k,j}^t | k = 1, 2, \dots, K\}$, $H = [h_0 \dots h_M]$ 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 value¹

$$T_{i,j}^{MTFM}$$



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

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...

$$f_1(x) = -x + 1$$

$$f_2(x) = \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \quad (8)$$

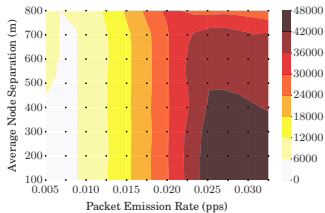
$$f_3(x) = x$$

► Back

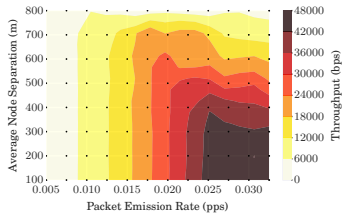
System Model Constraints

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

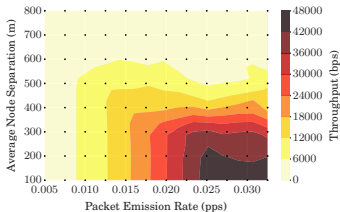
Throughput



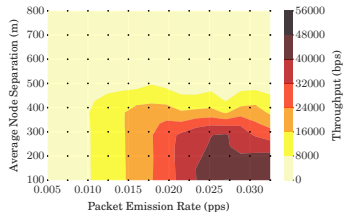
(a) Static



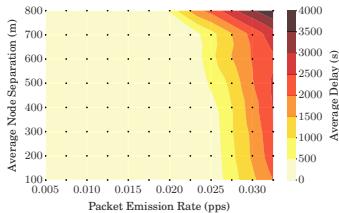
(b) Single Mobile



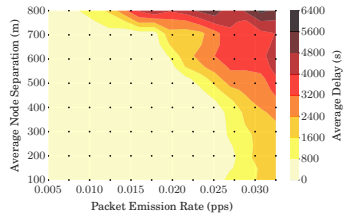
(c) All-but-one Mobile



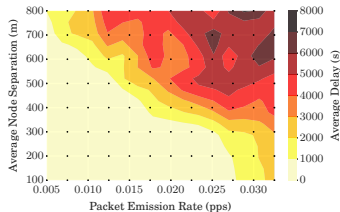
(d) All Mobile



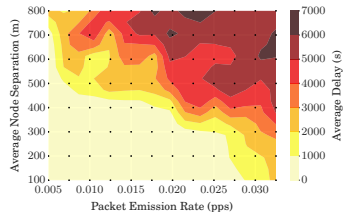
(a) Static



(b) Single Mobile

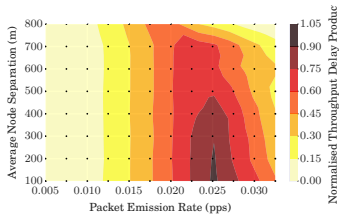


(c) All-but-one Mobile

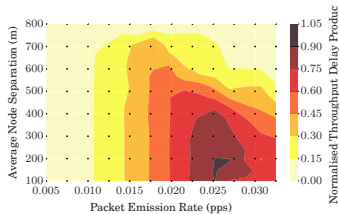


(d) All Mobile

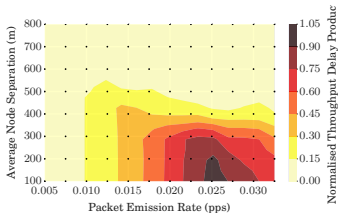
Fig 4.12: Normalised Throughput-Delay Product



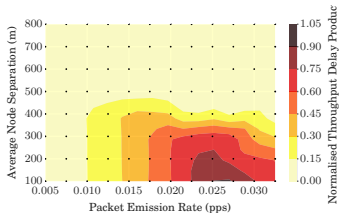
(a) Static



(b) Single Mobile

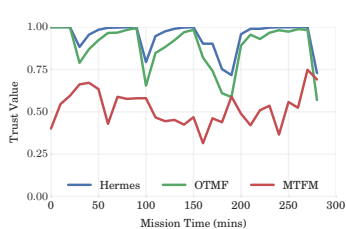


(c) All-but-one Mobile

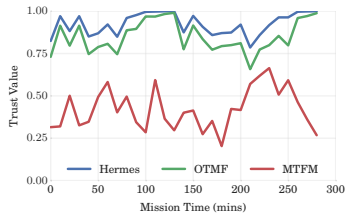


(d) All Mobile

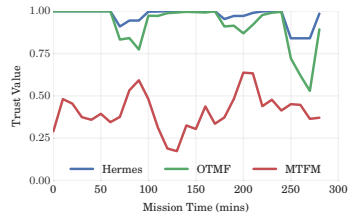
Fig 4.14: Hermes, OTMF, MTFM Trust assessments



(a) Fair Scenario



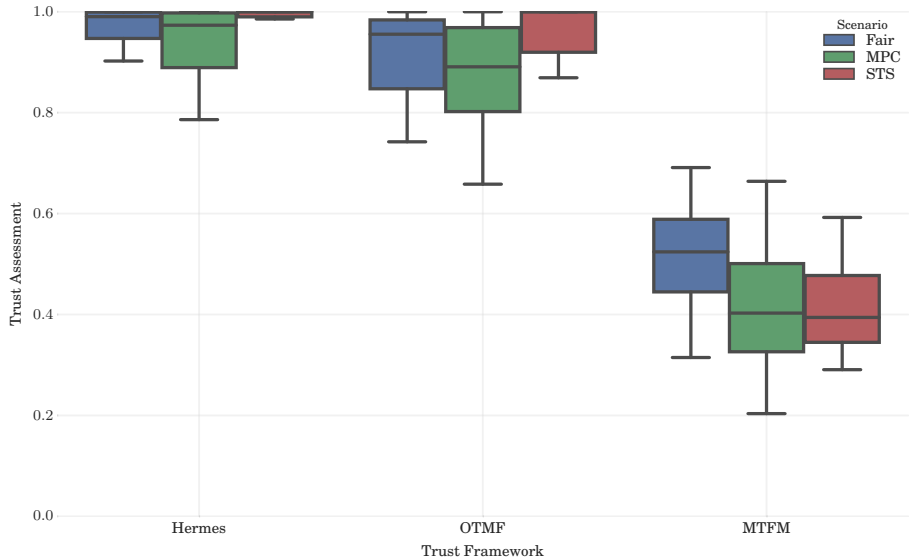
(b) Malicious Power Control (MPC) Scenario

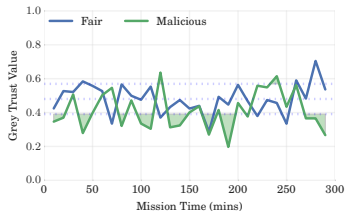


(c) Selfish Target Selection (STS) Scenario

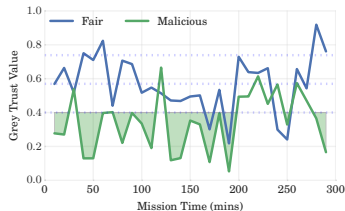
Fig. 9: $T_{0,1}$ for Hermes, OTMF, MTFM assessment values for fair and malicious behaviours in the fully mobile scenario

Fig. 4.15: Alternate Assessment Visualisation

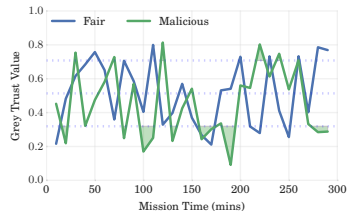




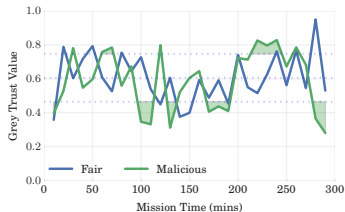
(a) Delay Emphasised



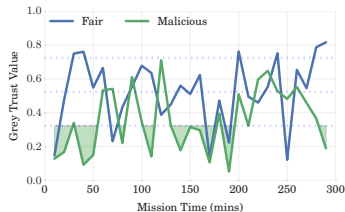
(b) PLR Emphasised



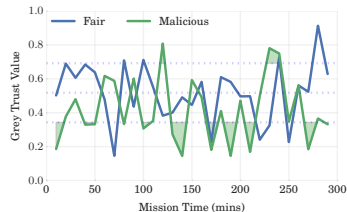
(c) Received Power (P_{RX}) Emphasised



(d) Transmit Power (P_{TX}) Emphasised



(e) Throughput (S) Emphasised



(f) Offered Load (G) Emphasised

Fig 4.18: Factor Analysis

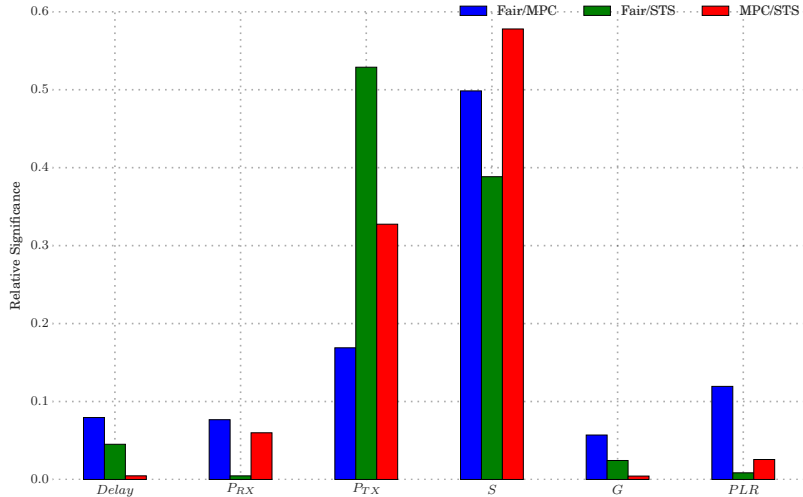


Fig. 12: Random Forest Factor Analysis of Malicious, Selfish and Fair behaviours compared against each-other

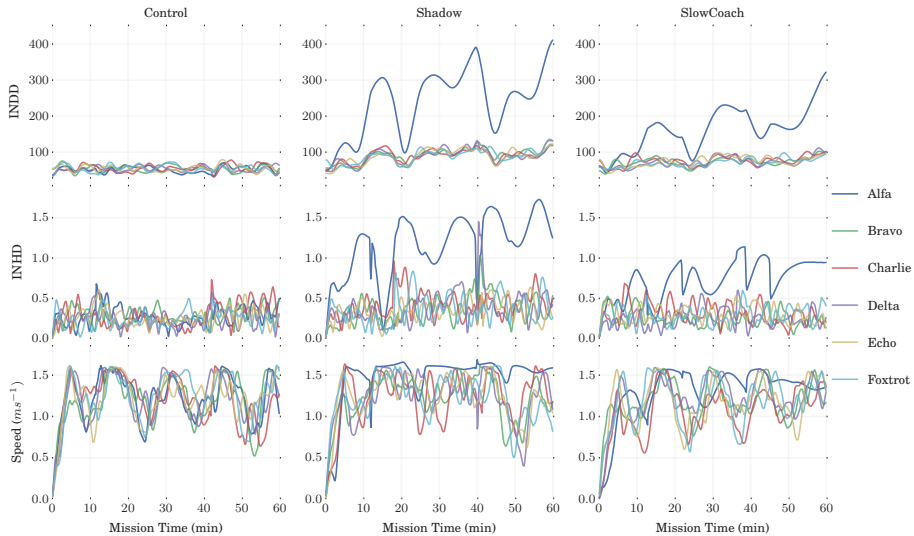


Fig. 13: Observed Metric Values for one simulation of each behaviour ($x_{i,j}^{m,t}$)

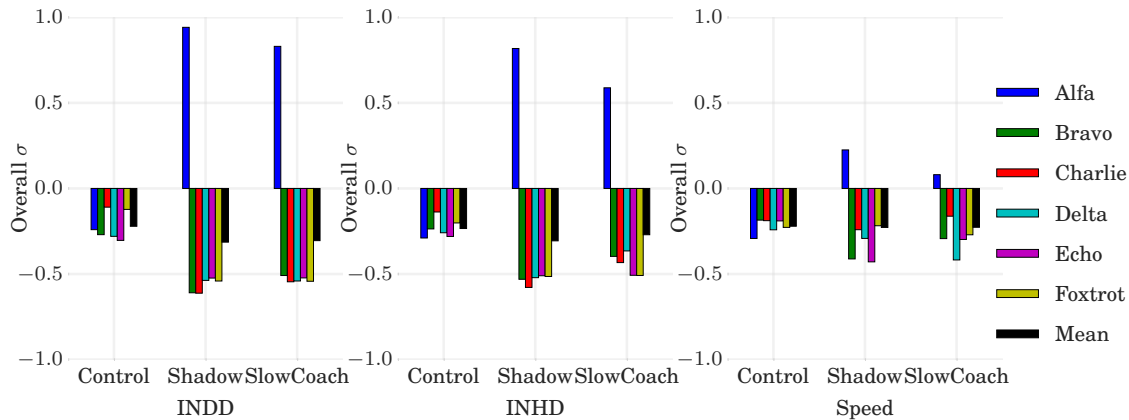


Fig. 14: Per-Node-Per-Run deviance for each metric, normalised in time ($\sum \alpha/T$)

Fig 6.1: Alternate Domain Construction

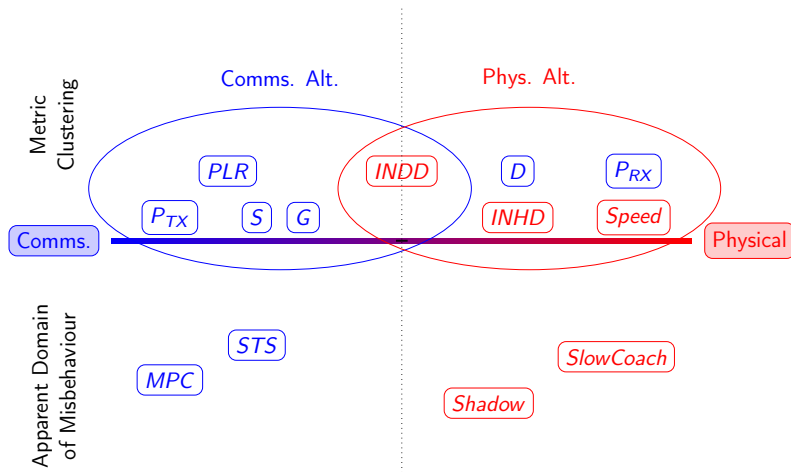


Fig. 15: Assumptions made about the relevant domains of impact / detectability of misbehaviours, and domain relevance of metrics, may not be optimal

Fig 6.2: Communications Metric Features

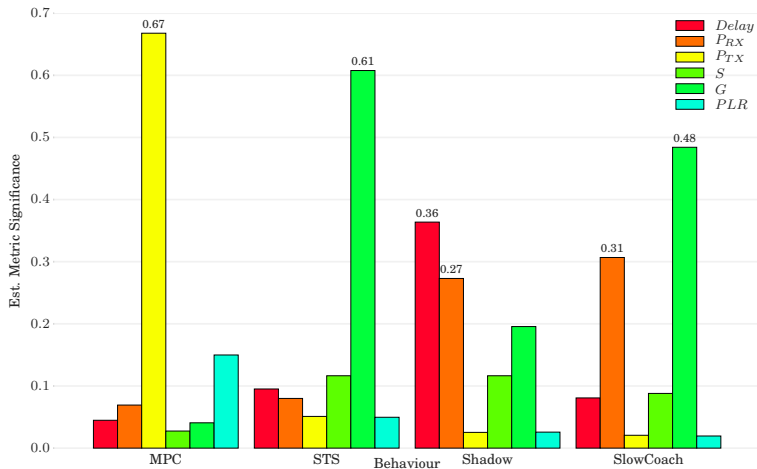


Fig. 16: Communications Metric Features (X_{comms})

Fig 6.3: Physical Metric Features

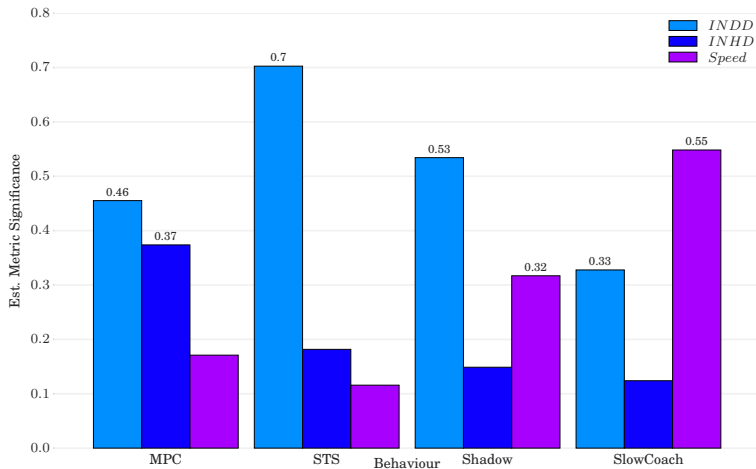


Fig. 17: Physical Metric Features (X_{phys})

Fig 6.4: Multi Domain Metric Features

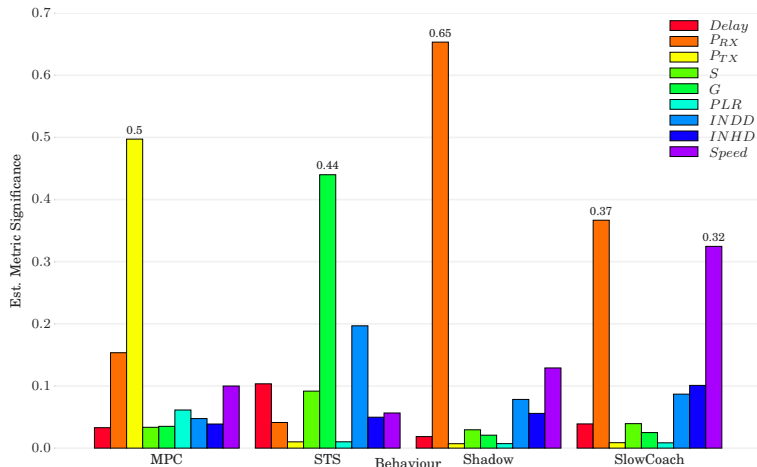
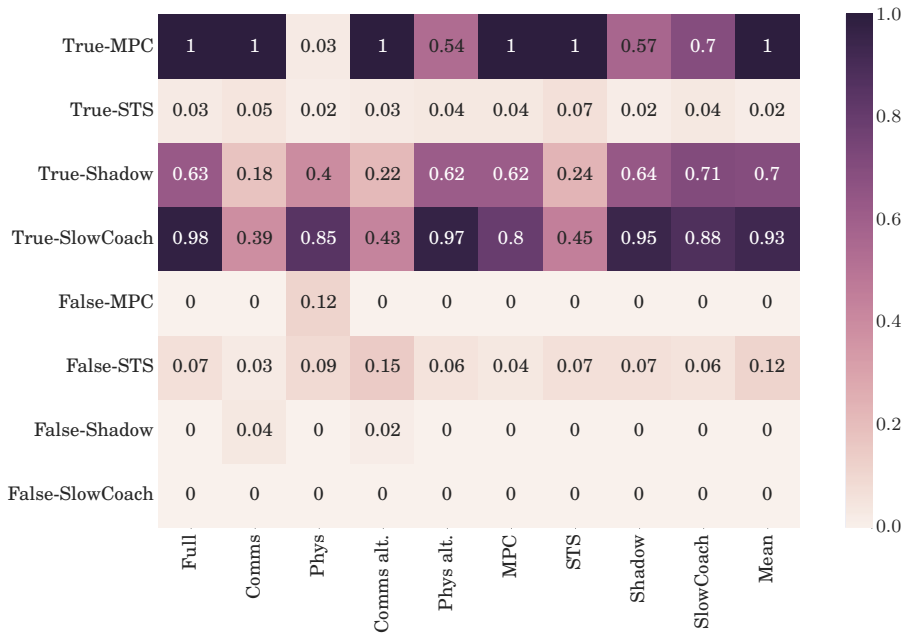


Fig. 18: Multi Domain Metric Features (X_{merge})

Table 2: Multi Domain Metric Feature Correlation (X_{merge})

	$Delay$	P_{RX}	P_{TX}	S	PLR	G	$INDD$	$INHD$	$Speed$
Misbehaviour									
MPC	-0.187	0.129	0.579	0.006	0.069	-0.146	0.040	-0.190	-0.297
STS	-0.195	-0.035	0.019	-0.100	0.019	0.381	-0.209	0.057	0.062
Shadow	0.004	-0.654	0.030	-0.016	0.030	0.063	0.120	0.158	0.266
SlowCoach	-0.157	-0.533	0.013	-0.132	0.013	-0.028	0.159	0.206	0.460

Positive Identification of Misbehavior-Target



Negative Identification of Misbehavior-Target

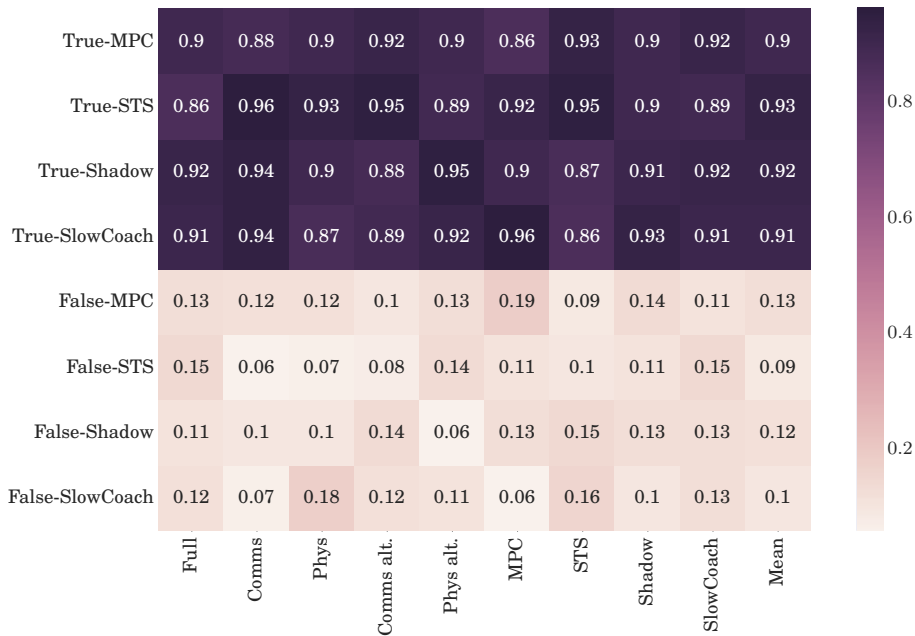


Table 3: ΔT_{ix} behaviour detection performance across meta-domains, including selected metrics

Domain		Behaviour ΔT_{ix}					Metrics in Domain								
		MPC	STS	Shadow	SlowCoach	Mean	Delay	P_{RX}	P_{TX}	S	G	PLR	INDD	INH	Speed
Basic	Full	0.81	-0.03	0.42	0.60	0.45	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Comms	0.85	0.04	0.19	0.26	0.34	✓	✓	✓	✓	✓	✓			
	Phys	0.04	0.00	0.39	0.69	0.28							✓	✓	✓
Alternate	Comms alt.	0.85	0.03	0.38	0.45	0.43				✓	✓	✓	✓		
	Phys alt.	0.48	0.03	0.42	0.63	0.39	✓	✓					✓	✓	✓
Synthetic	MPC	0.89	0.01	0.35	0.54	0.45	✓	✓	✓					✓	
	STS	0.86	0.06	0.37	0.49	0.45	✓		✓	✓		✓	✓		
	Shadow	0.49	-0.00	0.44	0.66	0.40		✓					✓	✓	✓
	SlowCoach	0.47	0.00	0.37	0.72	0.39	✓	✓		✓					✓
	Mean	0.88	0.03	0.42	0.69	0.50		✓	✓		✓		✓		✓

Fig 6.9. Metric-Target Correlations

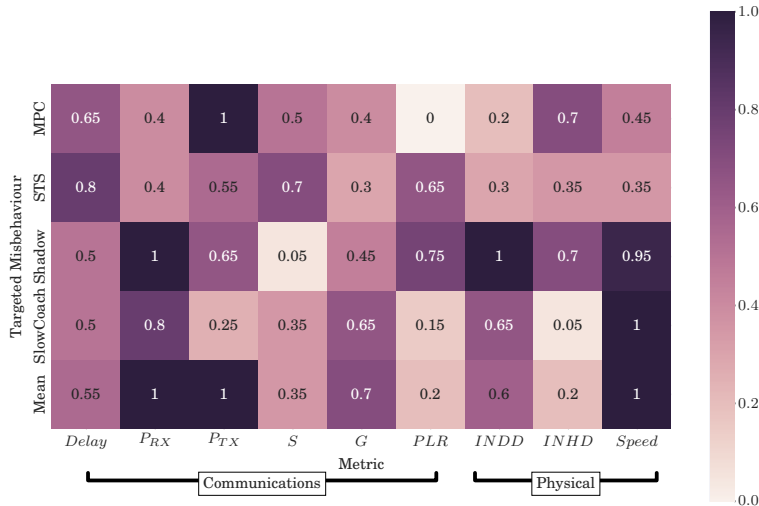
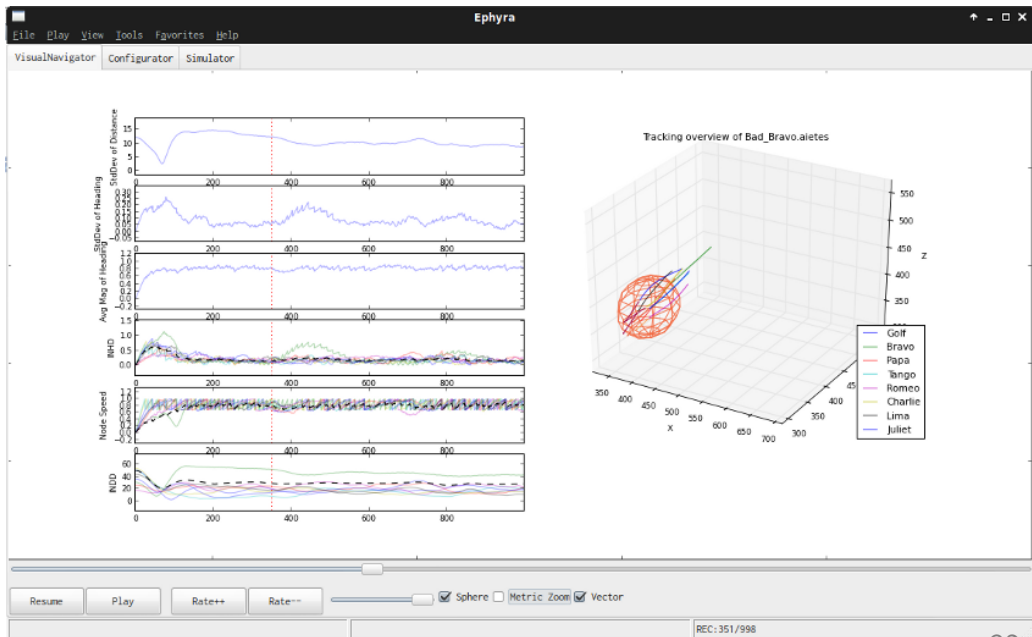


Fig. 21: Correlations between highest performing synthetic domain metrics with respect to Targeted misbehaviours



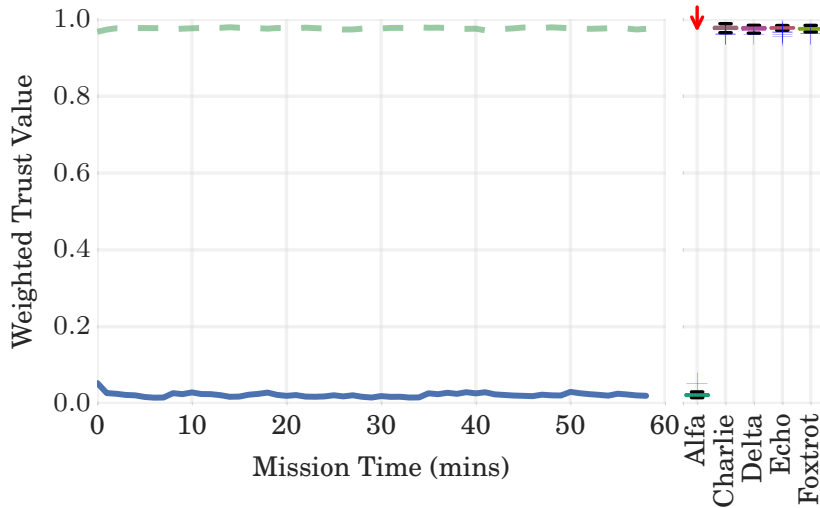


Fig. 22: MPC Comms Metric Shadow (showing mean of non-misbehaving nodes)

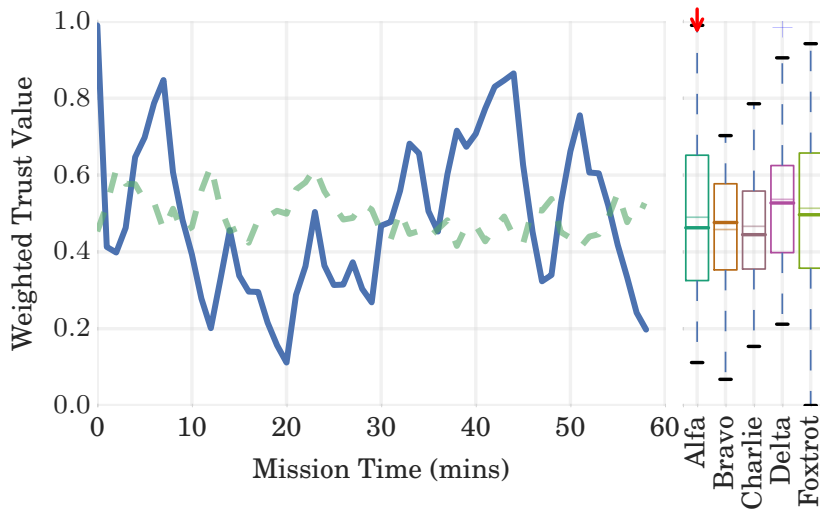


Fig. 23: MPC Physical Metric Shadow (showing mean of non-misbehaving nodes)

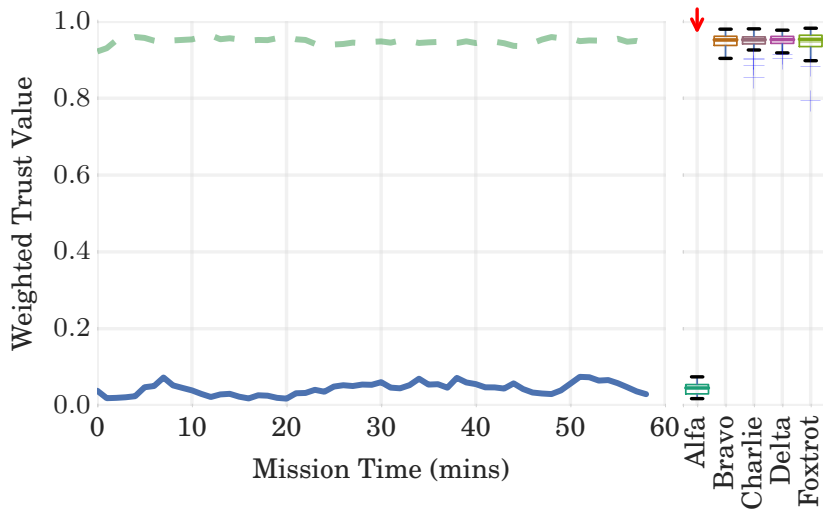


Fig. 24: MPC Full Metric Shadow (showing mean of non-misbehaving nodes)

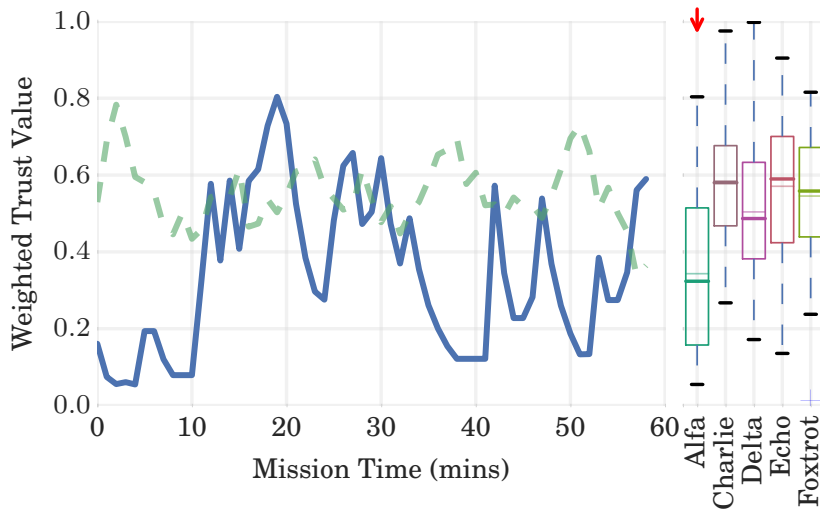


Fig. 25: STS Comms Metric Shadow (showing mean of non-misbehaving nodes)

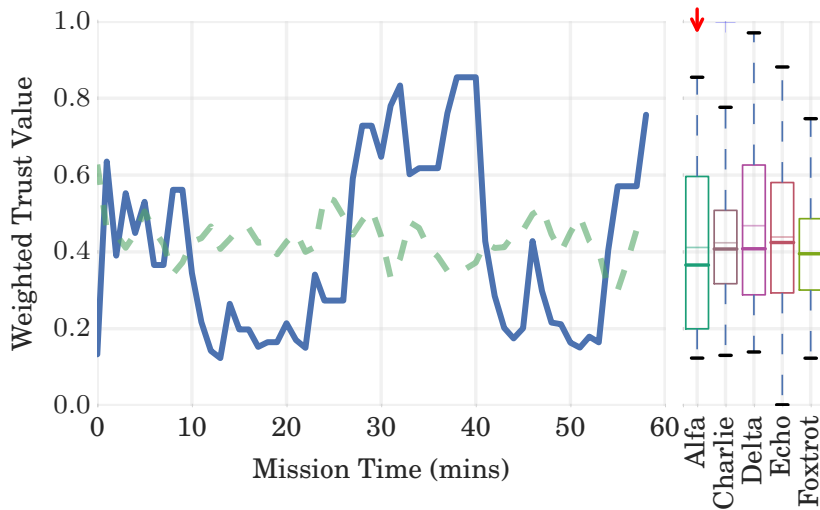


Fig. 26: STS Physical Metric Shadow (showing mean of non-misbehaving nodes)

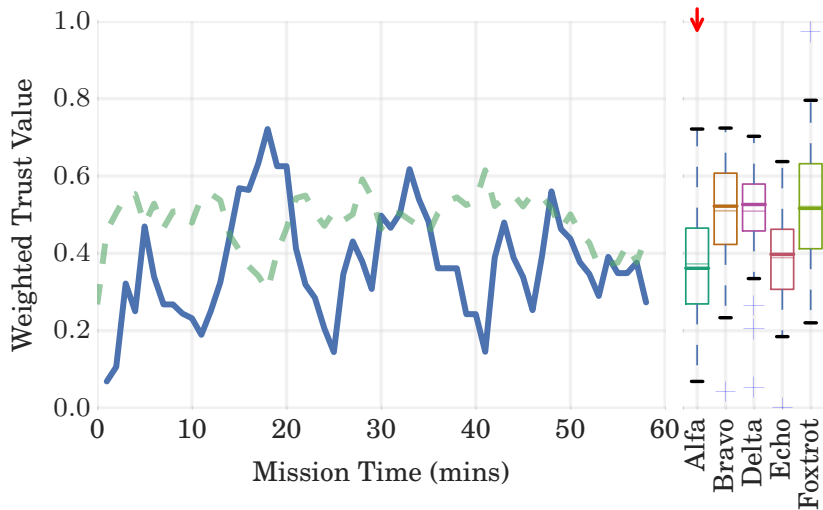


Fig. 27: STS Full Metric Shadow (showing mean of non-misbehaving nodes)

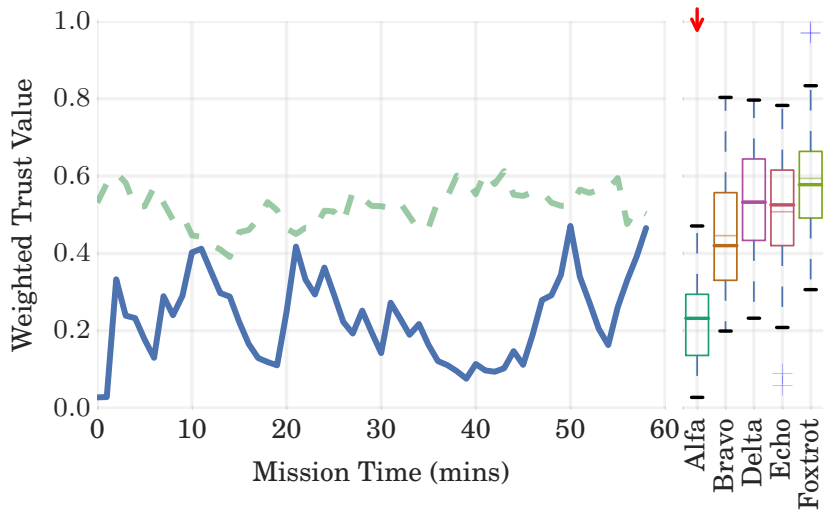


Fig. 28: Shadow Comms Metric Shadow (showing mean of non-misbehaving nodes)

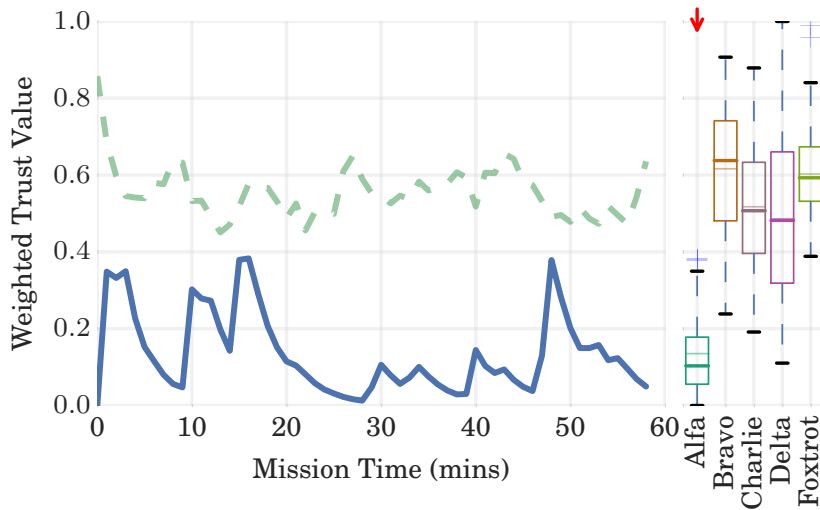


Fig. 29: Shadow Physical Metric Shadow (showing mean of non-misbehaving nodes)

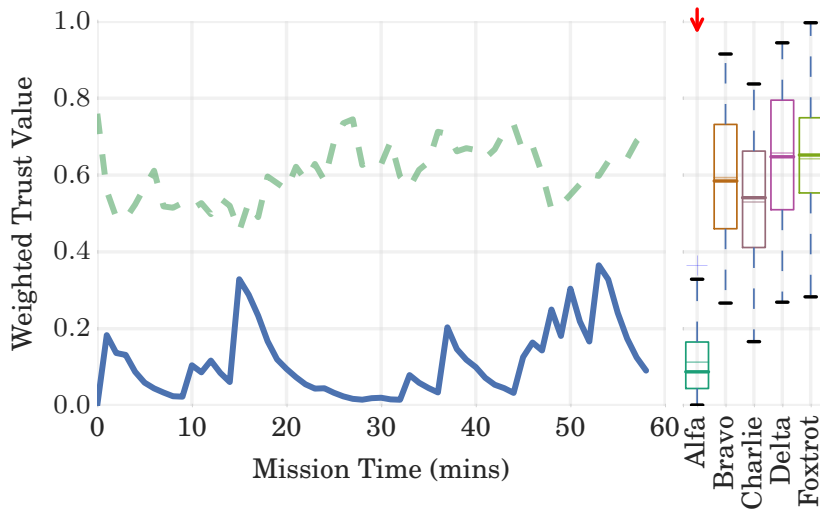


Fig. 30: Shadow Full Metric Shadow (showing mean of non-misbehaving nodes)

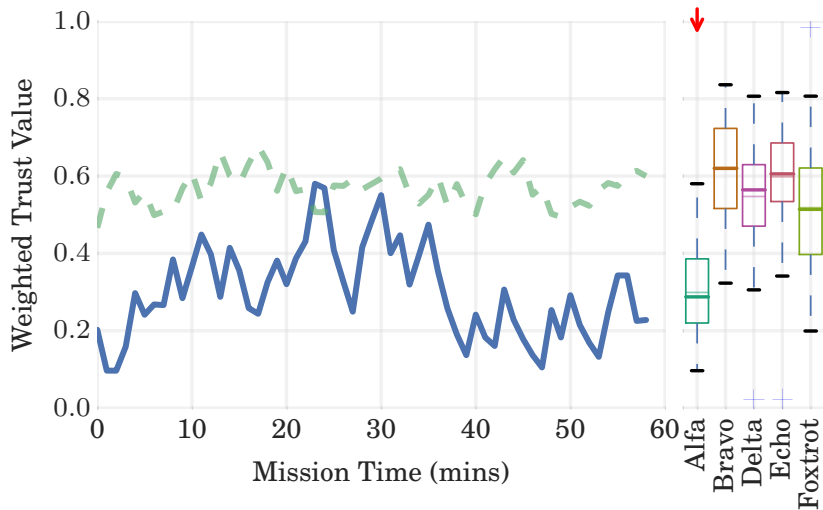


Fig. 31: SlowCoach Comms Metric Shadow (showing mean of non-misbehaving nodes)

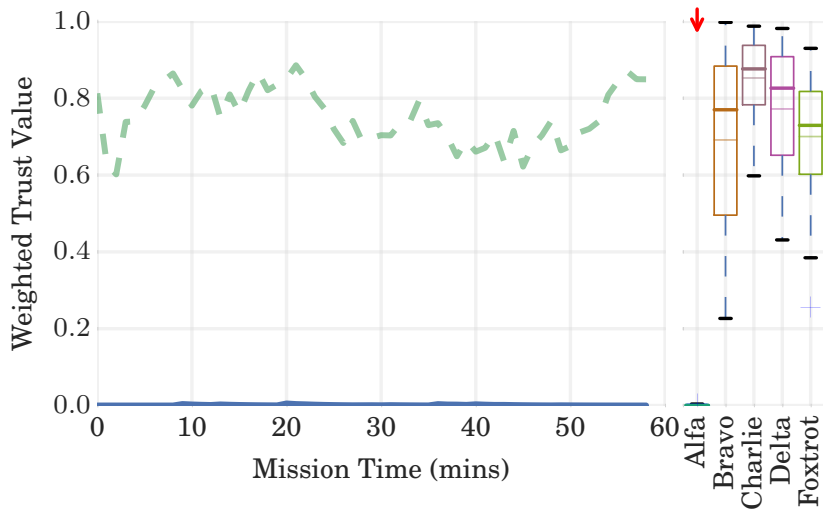


Fig. 32: SlowCoach Physical Metric Shadow (showing mean of non-misbehaving nodes)

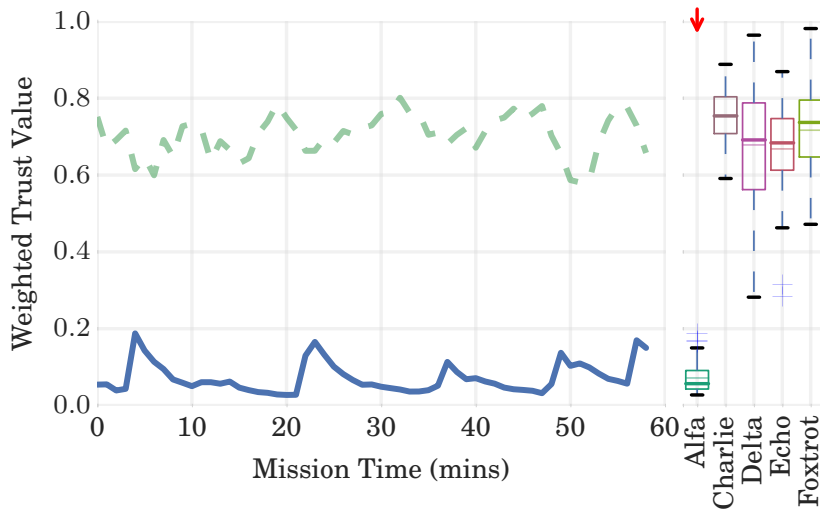


Fig. 33: SlowCoach Full Metric Shadow (showing mean of non-misbehaving nodes)

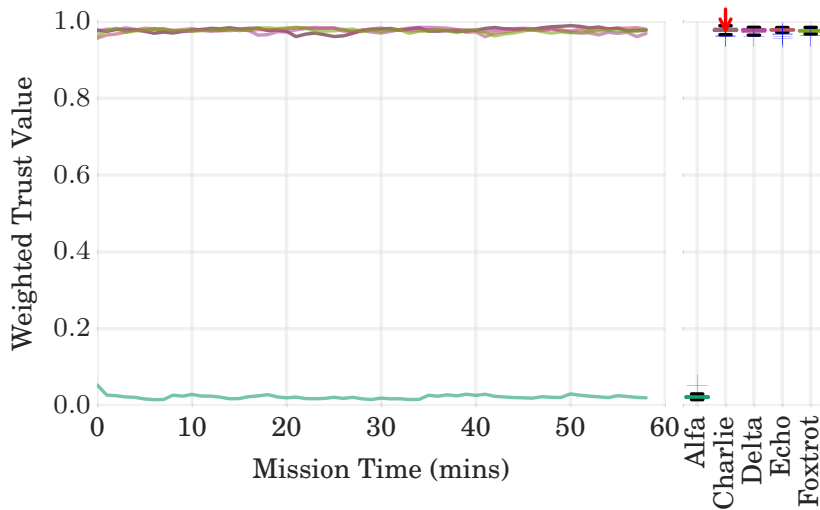


Fig. 34: MPC Comms Metric Shadow (targeting non-malicious node)

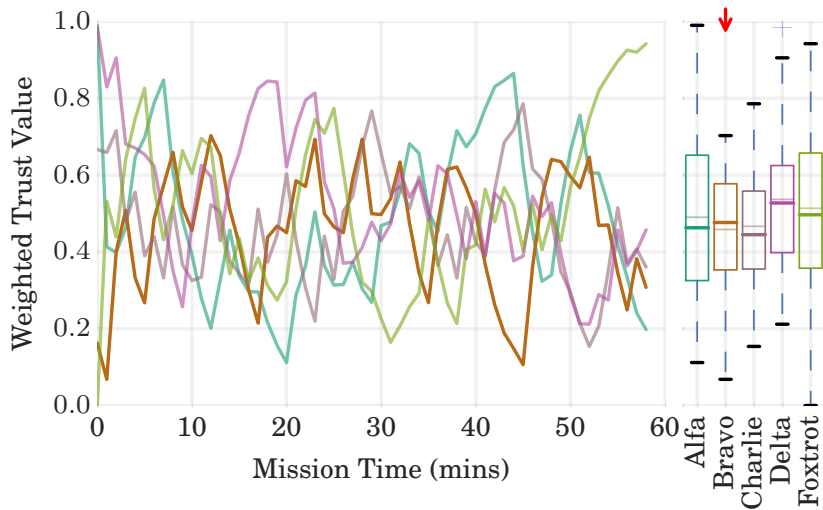


Fig. 35: MPC Physical Metric Shadow (targeting non-malicious node)

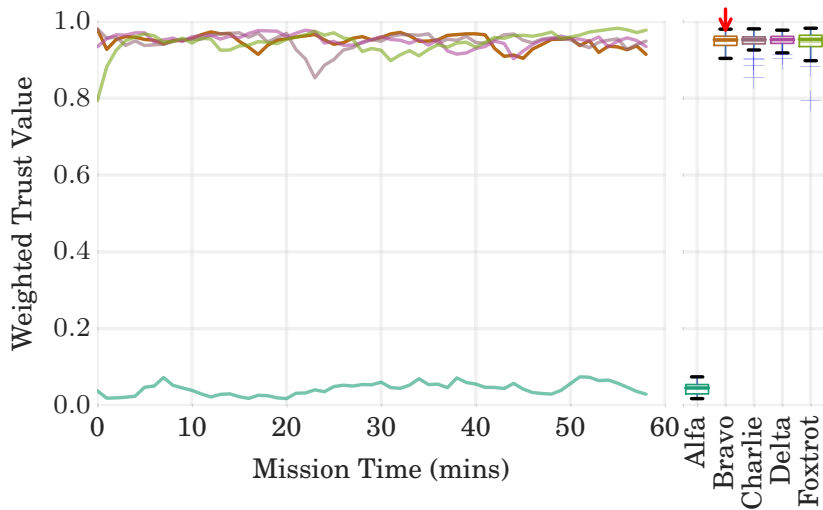


Fig. 36: MPC Full Metric Shadow (targeting non-malicious node)

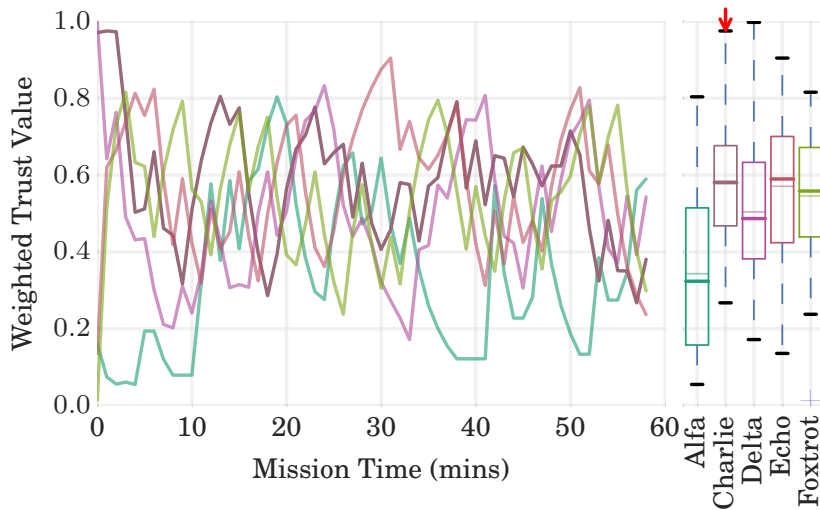


Fig. 37: STS Comms Metric Shadow (targeting non-malicious node)

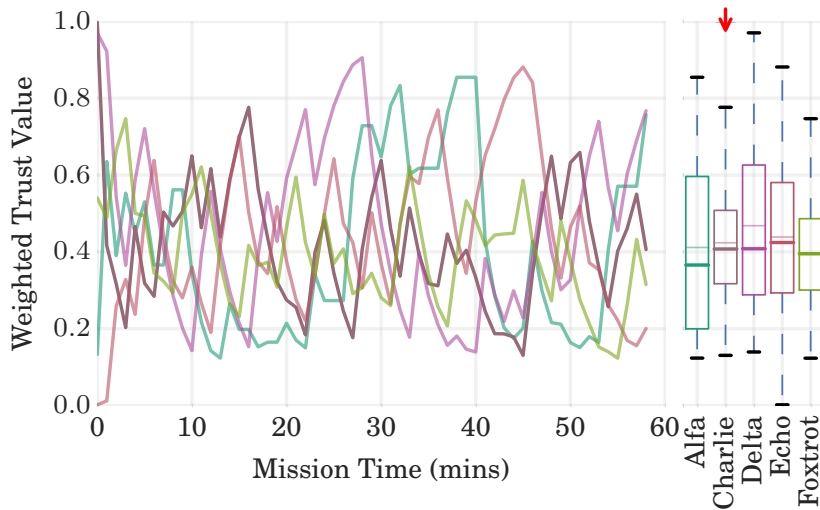


Fig. 38: STS Physical Metric Shadow (targeting non-malicious node)

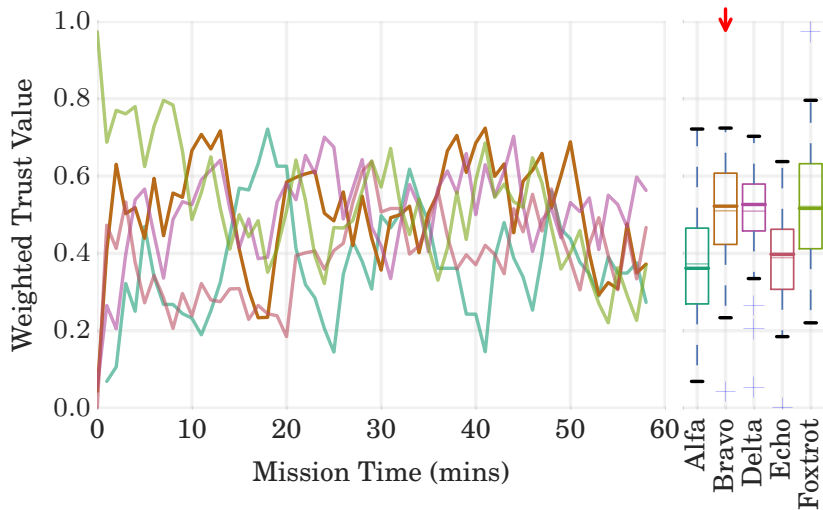


Fig. 39: STS Full Metric Shadow (targeting non-malicious node)

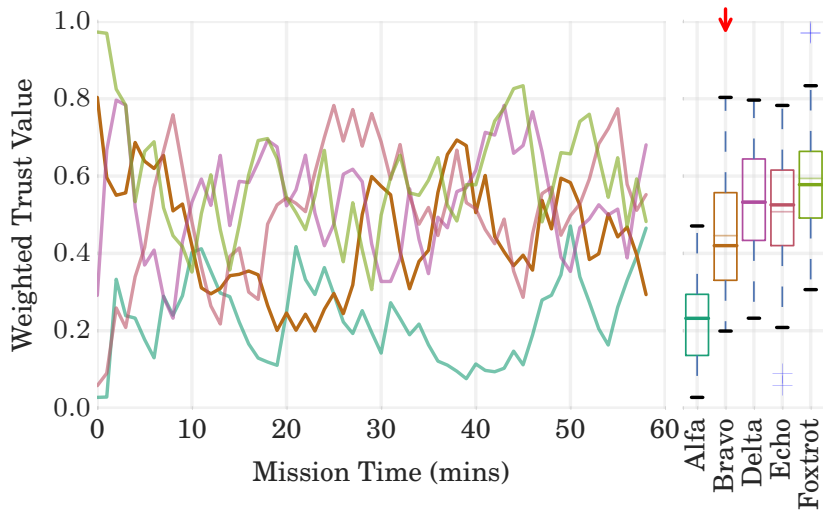


Fig. 40: Shadow Comms Metric Shadow (targeting non-malicious node)

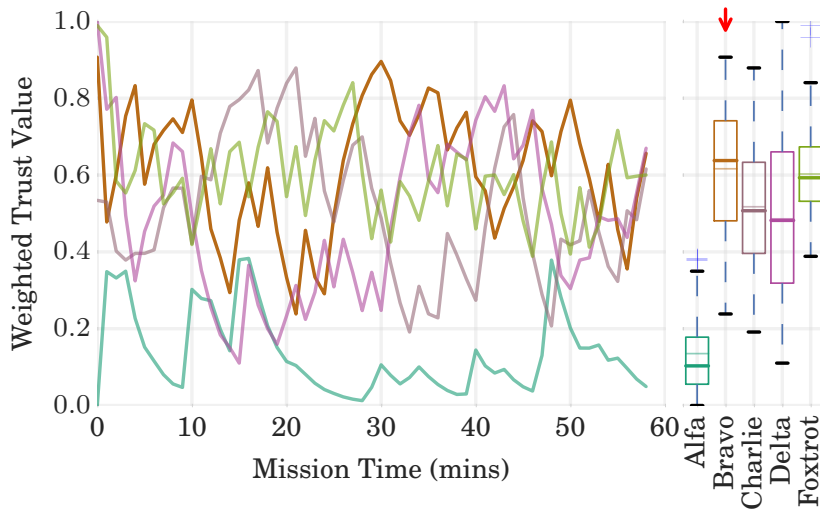


Fig. 41: Shadow Physical Metric Shadow (targeting non-malicious node)

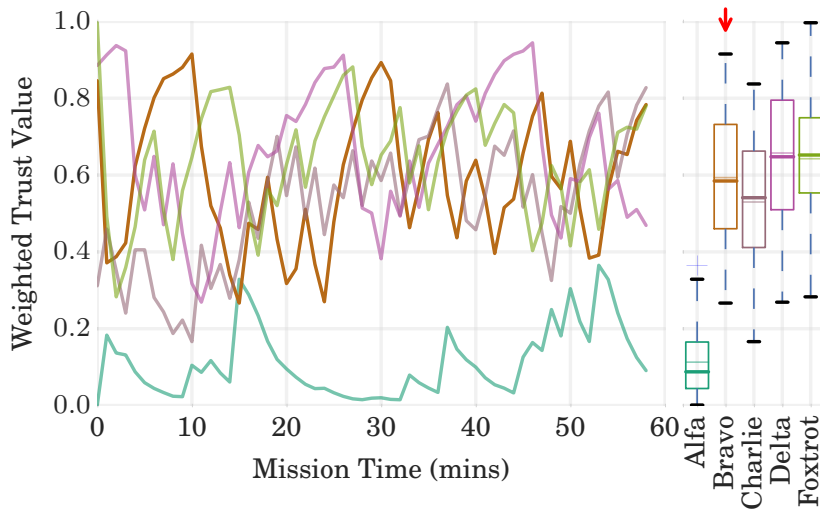


Fig. 42: Shadow Full Metric Shadow (targeting non-malicious node)

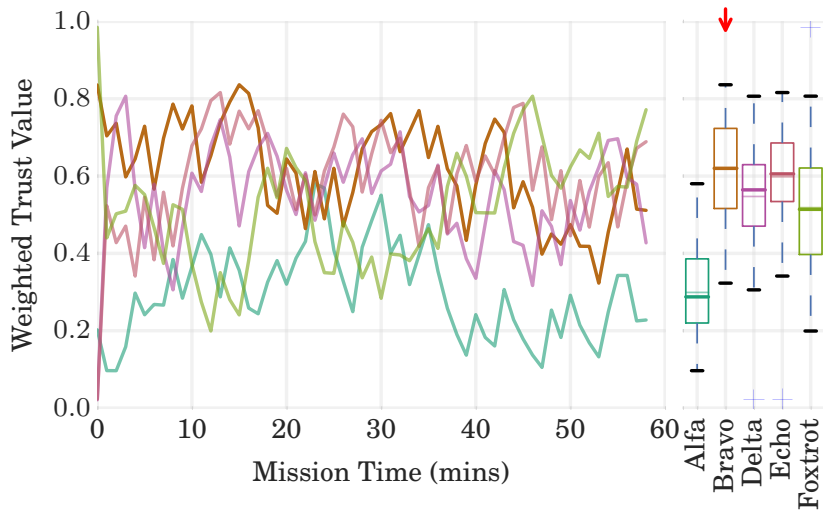


Fig. 43: SlowCoach Comms Metric Shadow (targeting non-malicious node)

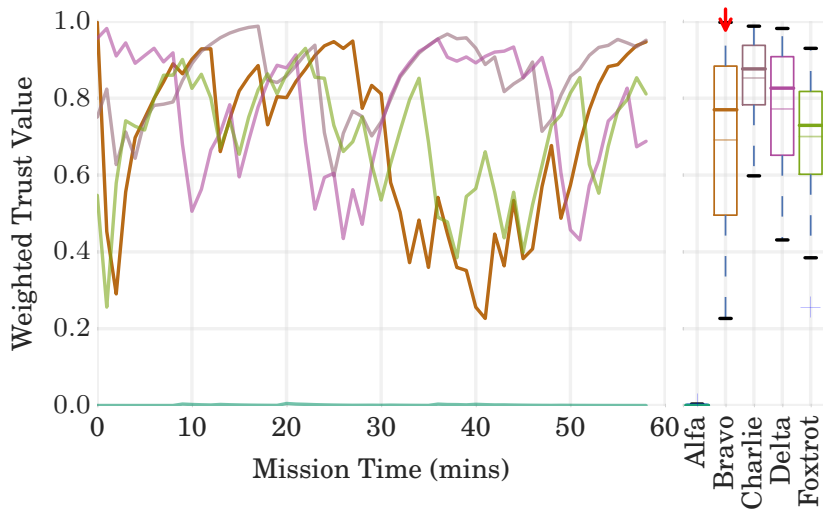


Fig. 44: SlowCoach Physical Metric Shadow (targeting non-malicious node)

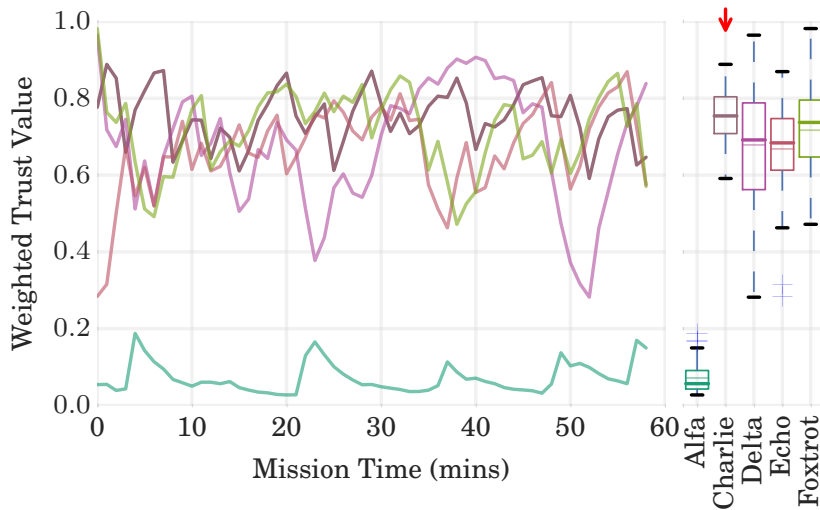


Fig. 45: SlowCoach Full Metric Shadow (targeting non-malicious node)

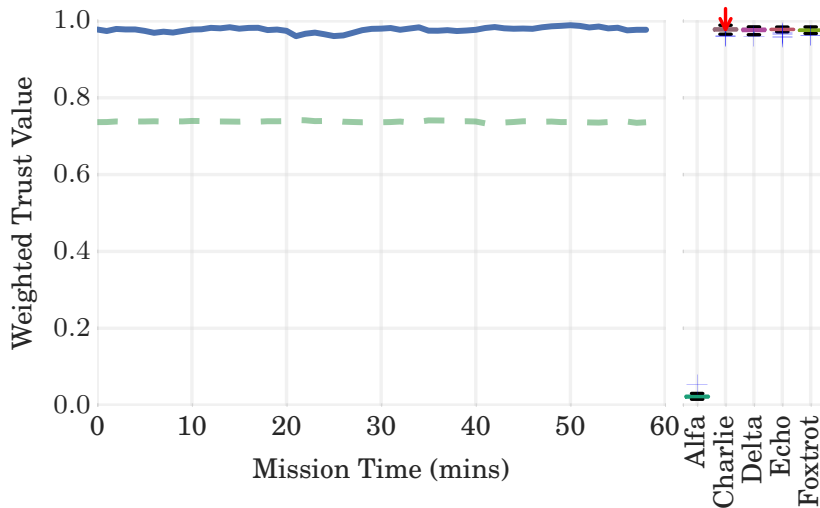


Fig. 46: MPC Comms Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

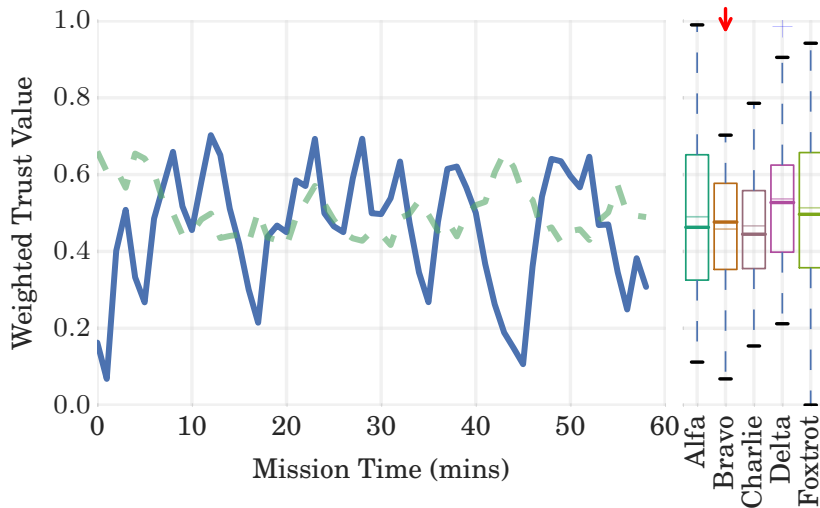


Fig. 47: MPC Physical Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

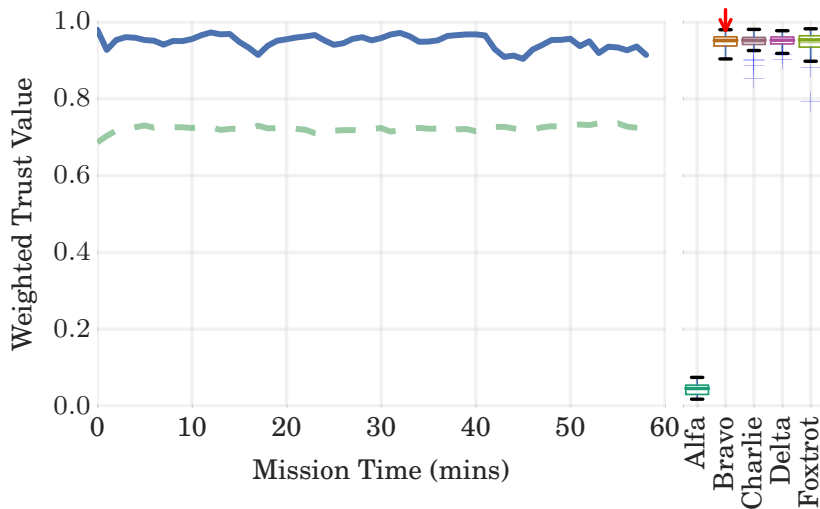


Fig. 48: MPC Full Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

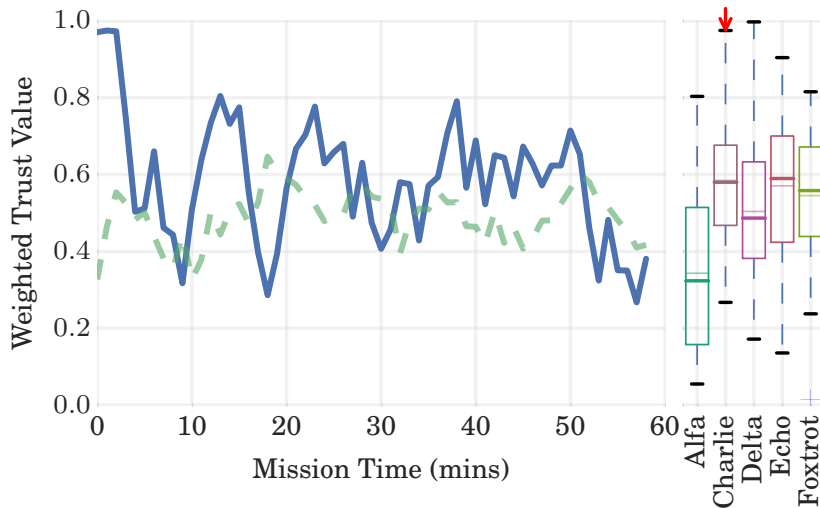


Fig. 49: STS Comms Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

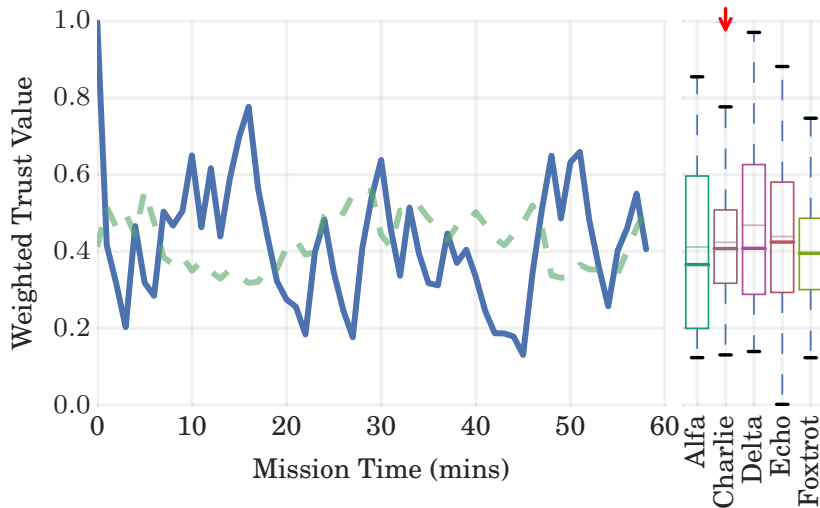


Fig. 50: STS Physical Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

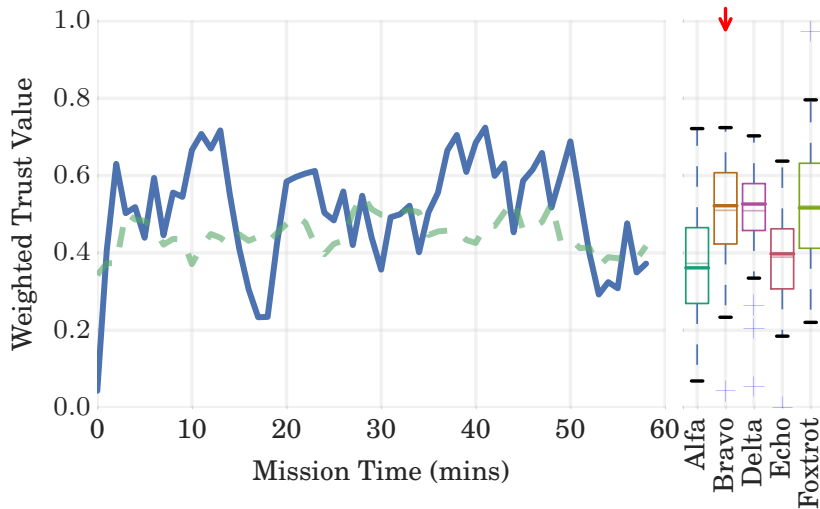


Fig. 51: STS Full Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

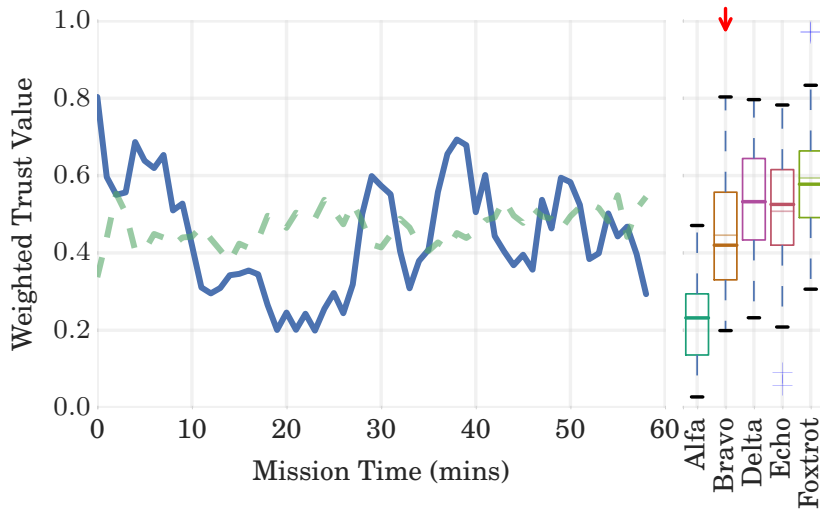


Fig. 52: Shadow Comms Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

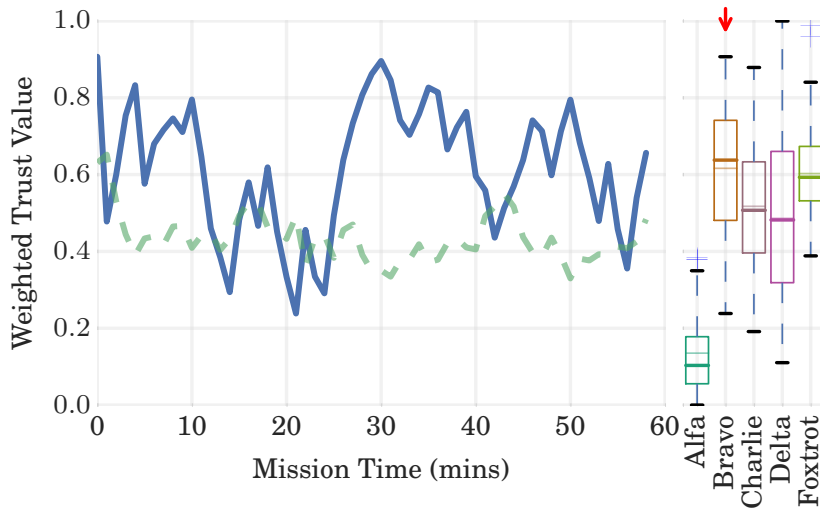


Fig. 53: Shadow Physical Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

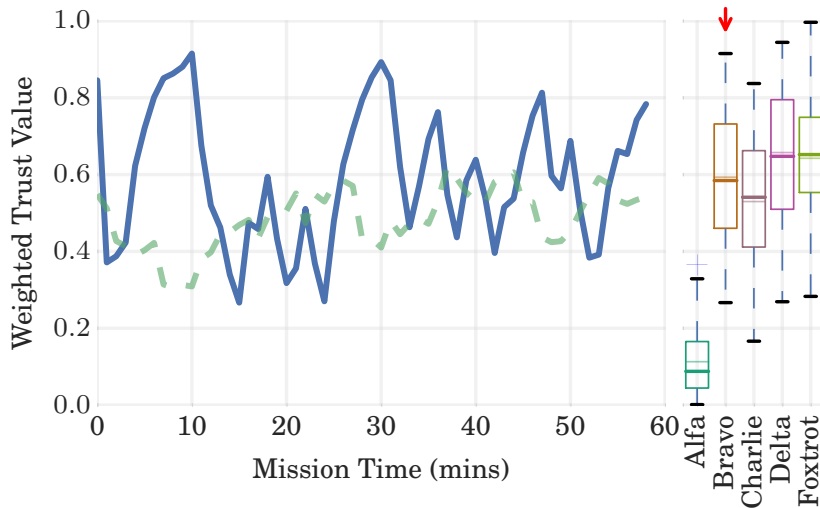


Fig. 54: Shadow Full Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

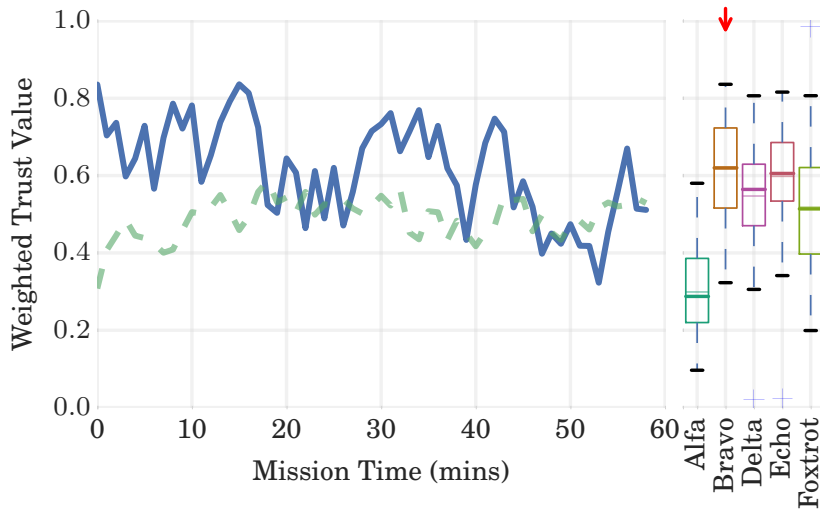


Fig. 55: SlowCoach Comms Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

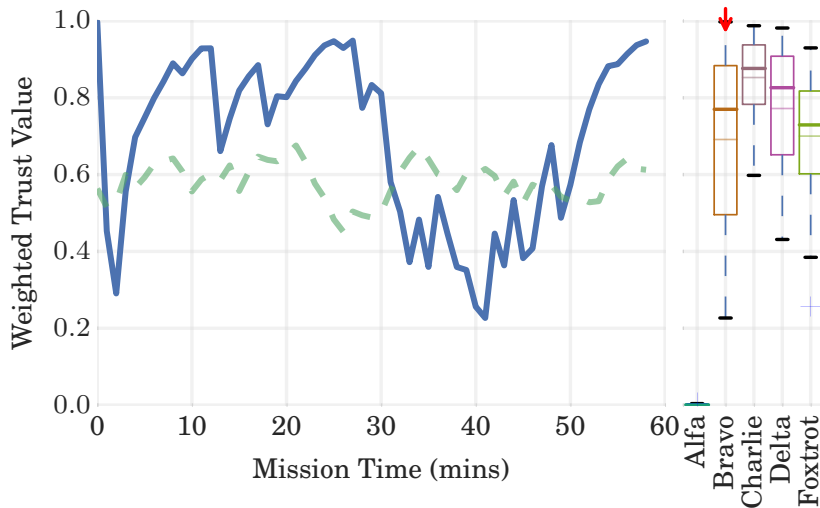


Fig. 56: SlowCoach Physical Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)

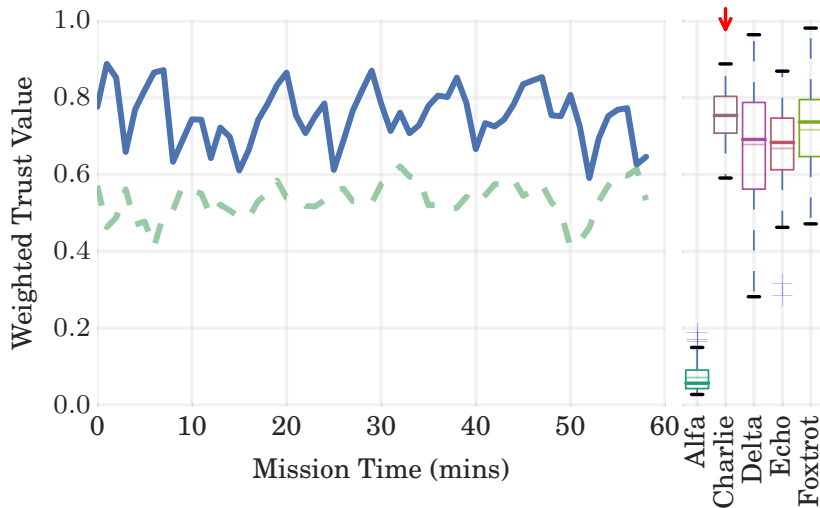


Fig. 57: SlowCoach Full Metric Shadow (targeting non-malicious node, showing mean of remaining cohort including malicious node)