A Multi-Vector Trust Framework for Autonomous Systems

Andrew Bolster, Alan Marshall

University of Liverpool

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

March 24, 2014

Trust in Ad-Hoc Systems and the context of this document

- Particularly interested in the application of Trust in Decentralised (P2P) Autonomous Systems of Systems, Autonomous Underwater Vehicles (AUVs) for example

Trust in Ad-Hoc Systems and the context of this document

- Particularly interested in the application of Trust in Decentralised (P2P) Autonomous Systems of Systems, Autonomous Underwater Vehicles (AUVs) for example
- Trust: *The expectation of an actor performing a certain task or range of tasks within a certain confidence or probability*

Trust in Ad-Hoc Systems and the context of this document

- Particularly interested in the application of Trust in Decentralised (P2P) Autonomous Systems of Systems, Autonomous Underwater Vehicles (AUVs) for example
- Trust: *The expectation of an actor performing a certain task or range of tasks within a certain confidence or probability*
- Full System Views of Trust
  - Design Trust - that a system of systems will perfom as spec'd / designed in operation

Trust in Ad-Hoc Systems and the context of this document

- Particularly interested in the application of Trust in Decentralised (P2P) Autonomous Systems of Systems, Autonomous Underwater Vehicles (AUVs) for example
- Trust: *The expectation of an actor performing a certain task or range of tasks within a certain confidence or probability*
- Full System Views of Trust
  - Design Trust - that a system of systems will perfom as spec'd / designed in operation
  - Operational Trust - the systems within a larger system will perfom as designed in field ✓

Trust Management Frameworks

- Provide information regarding the estimated future states and operations of nodes within networks

[1] Huaizhi Li and Mukesh Singhal. "Trust Management in Distributed Systems". In: *Computer (Long. Beach. Calif).* 40.2 (2007), pp. 45–53. ISSN: 00189162. DOI: 10.1109/MC.2007.76. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622.

Trust Management Frameworks

- Provide information regarding the estimated future states and operations of nodes within networks
- "[. . .]collecting the information necessary to establish a trust relationship and dynamically monitoring and adjusting the existing trust relationship" -[1]

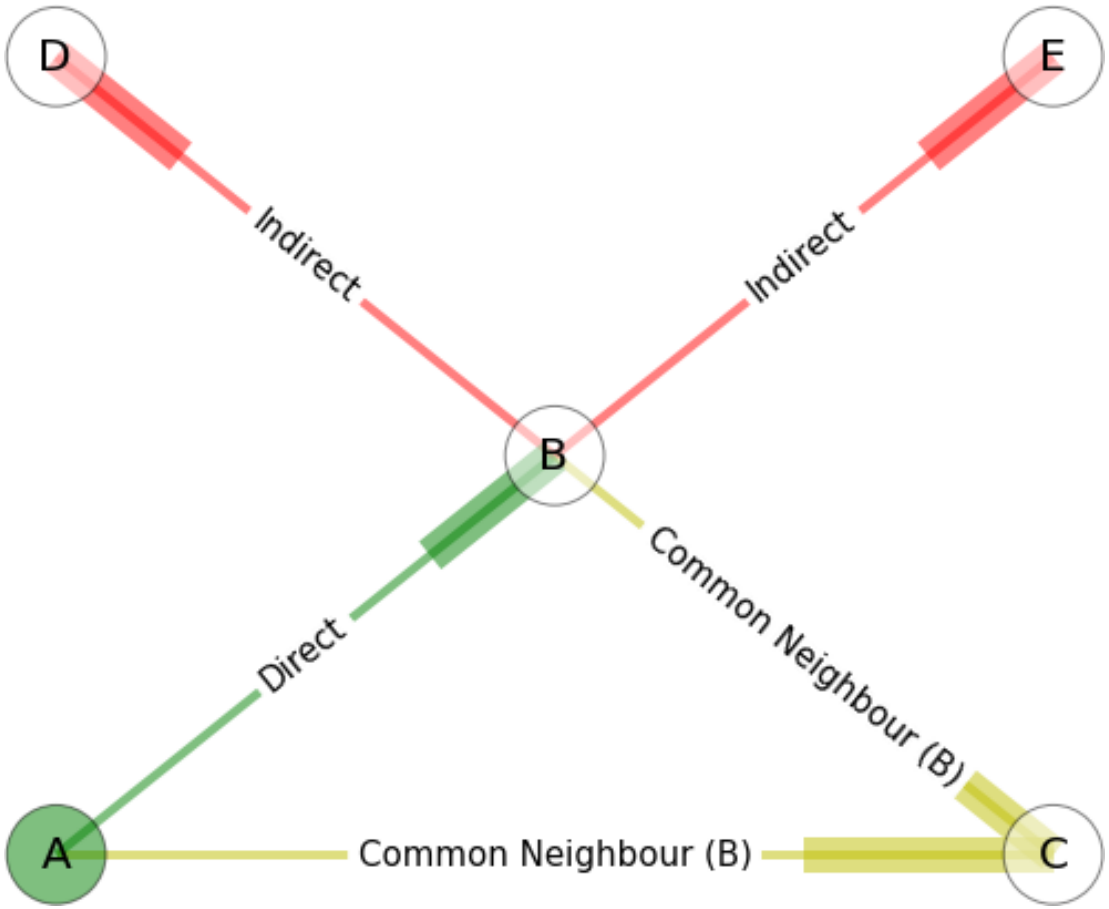
[1] Huaizhi Li and Mukesh Singhal. "Trust Management in Distributed Systems". In: *Computer (Long. Beach. Calif).* 40.2 (2007), pp. 45–53. ISSN: 00189162. DOI: 10.1109/MC.2007.76. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622.

Trust Management Frameworks

- Provide information regarding the estimated future states and operations of nodes within networks
- "[. . .]collecting the information necessary to establish a trust relationship and dynamically monitoring and adjusting the existing trust relationship" -[1]
- Enables nodes to form collaborative *opinions* on their cohort nodes based on
  - Direct Observation of Communications Behaviour (eg Successfully Forwarded Packets)
  - Common-Neighbour Recommendation
  - Indirect Reputation

[1] Huaizhi Li and Mukesh Singhal. "Trust Management in Distributed Systems". In: *Computer (Long. Beach. Calif).* 40.2 (2007), pp. 45–53. ISSN: 00189162. DOI: 10.1109/MC.2007.76. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622.

Transitivity in Trust Networks



TMFs in Ad Hoc Autonomous Systems

- Multiple transitive relationships can be maintained over time, providing trust resilience with dyanmic network topology

TMFs in Ad Hoc Autonomous Systems

- Multiple transitive relationships can be maintained over time, providing trust resilience with dyanmic network topology
- Enable trust establishment from partial-strangers via indirect trust and direct observation

TMFs in Ad Hoc Autonomous Systems

- Multiple transitive relationships can be maintained over time, providing trust resilience with dyanmic network topology
- Enable trust establishment from partial-strangers via indirect trust and direct observation
- Enables nodes to inform internal processes for global efficiency given observed network behaviour / 'wellness', similar to those found in human social networks eg
  - Update routing table based on 'safest' node chains (Phone Tree)
  - Maneuver away from misbehaving nodes (Shunning)
  - Inform as to 'trustworthiness' of forwarded information (Healthy sense of Skepticism)
  - Historic Distrust/Trust decaying over time (Forgiveness/Relationship Decay)

Reason for using TMFs in MANETs

- Provide Risk Mitigation against many classical MANET attacks
  - Black/Grayhole
  - Routing Loop
  - Selective misbehaviour / selfishness
- Generally; to constrain potential malicious behaviour that can operate without detection

Trust in Autonomous Systems

- Public Key Infrastructure - Requires Centralised Control and pre-shared keys
- Resurrecting Duckling - Uses in-action keying with a trusted source
- Evidence Based Trust - Uses shared keys
- Reputation Based Trust - Uses Packet forwarding success rate for prediction of future actions
  - CONFIDANT - Trust-based router implementation using packet forwarding rate
  - OTMF - Trust including transitive information from otehr nodes

- . . . and there are plenty more along the same lines

Trust in Autonomous Systems

- Public Key Infrastructure - Requires Centralised Control and pre-shared keys
- Resurrecting Duckling - Uses in-action keying with a trusted source
- Evidence Based Trust - Uses shared keys
- Reputation Based Trust - Uses Packet forwarding success rate for prediction of future actions
  - CONFIDANT - Trust-based router implementation using packet forwarding rate
  - OTMF - Trust including transitive information from otehr nodes
  - MTMF - Relationships and Multiple Metrics combined with Gray Interval assessment
- . . . and there are plenty more along the same lines

Vectorised Trust

- Application of several individual metrics for the construction of a single trust measurement
- For example:
  - $X = \{packet\ loss, signal\ strength, datarate, delay, throughput\}$
- This multi-parameter trust prevents 'smart' attackers; leveraging a known trust metric to subvert a TMF without detection
- Normally expressed as a vector, but can be condensed into an abstracted or weighted form for comparison [1]

Gray Theory and it's Application in MTMF

- $\left[\theta_{k,j}, \phi_{k,j}\right]^t = \left[\frac{\min_k |a_{kj}^t - g_j^t| + \rho \max_k |a_{kj}^t - g_j^t|}{\max_k |a_{kj}^t - g_j^t| t}, \frac{\min_k |a_{kj}^t - b_j^t| + \rho \max_k |a_{kj}^t - b_j^t|}{\max_k |a_{kj}^t - b_j^t| t}\right]$ [3]
- Basically, scale the individual values against the global maximum and minimum of the sample set to obtain an interval

Gray Theory and it's Application in MTMF

- $\left[\theta_{k,j}, \phi_{k,j}\right]^t = \left[\frac{\min_k |a_{kj}^t - g_j^t| + \rho \max_k |a_{kj}^t - g_j^t|}{\max_k |a_{kj}^t - g_j^t| t}, \frac{\min_k |a_{kj}^t - b_j^t| + \rho \max_k |a_{kj}^t - b_j^t|}{\max_k |a_{kj}^t - b_j^t| t}\right]$ [3]
- Basically, scale the individual values against the global maximum and minimum of the sample set to obtain an interval
- $\left[\theta_k, \phi_k\right]^t = \sum_{j=1}^{m} h_j \left[\theta_{k,j}^t, \phi_{k,j}^t\right]$

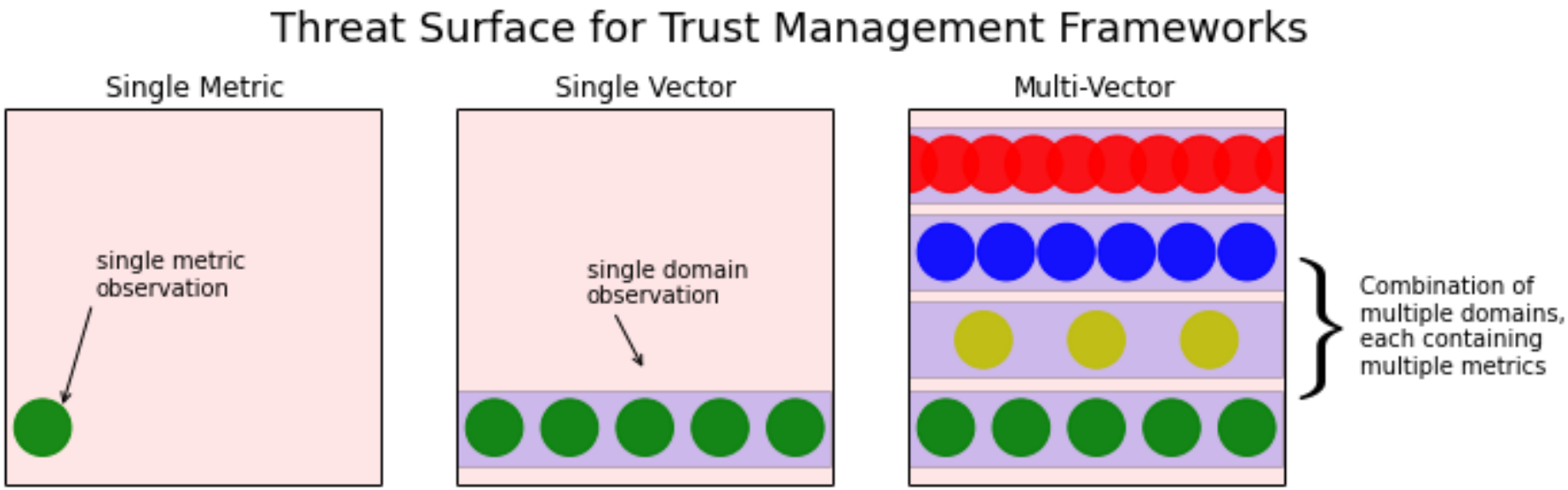
Gray Theory and it's Application in MTMF

- $\left[\theta_{k,j}, \phi_{k,j}\right]^t = \left[\frac{\min_k |a_{kj}^t - g_j^t| + \rho \max_k |a_{kj}^t - g_j^t|}{\max_k |a_{kj}^t - g_j^t| t}, \frac{\min_k |a_{kj}^t - b_j^t| + \rho \max_k |a_{kj}^t - b_j^t|}{\max_k |a_{kj}^t - b_j^t| t}\right]$ [3]
- Basically, scale the individual values against the global maximum and minimum of the sample set to obtain an interval
- $\left[\theta_k, \phi_k\right]^t = \sum_{j=1}^{m} h_j \left[\theta_{k,j}^t, \phi_{k,j}^t\right]$
- $T_k^t = \frac{1}{1 + \frac{(\phi_k^t)^2}{(\theta_k^t)^2}}$

  $\mathrm{T}_{k,tot}^t = T_k^t + T_{k,net}^t + (\alpha \times T_k^{t-1} + (1 - \alpha) \times T_{k,tot}^{t-1})$

Multi-Vector Trust and the Threat Surface

Potential attacks exist across a multi-domain threat surface



Trust in Mobile Autonomous Underwater Vehicles

- Flocking with Intent: MCM, Port Protection, Survey, Protection Detail, etc.

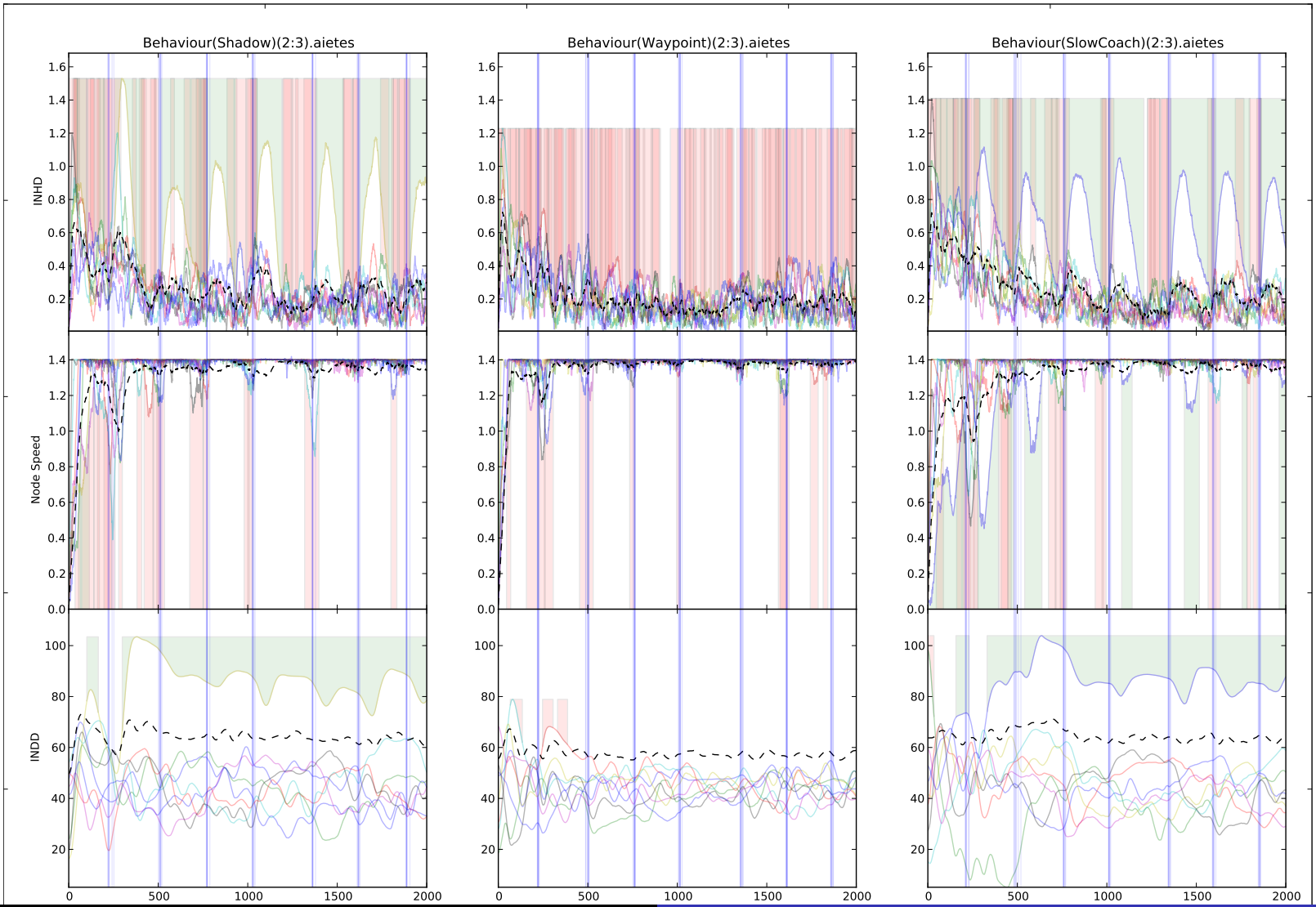
Trust in Mobile Autonomous Underwater Vehicles

- Flocking with Intent: MCM, Port Protection, Survey, Protection Detail, etc.
- Metric Selection in collaboration CMRE/DSTL
  - Inter Node Heading Deviation
  - Inter Node Distance Deviation
  - Node Speed

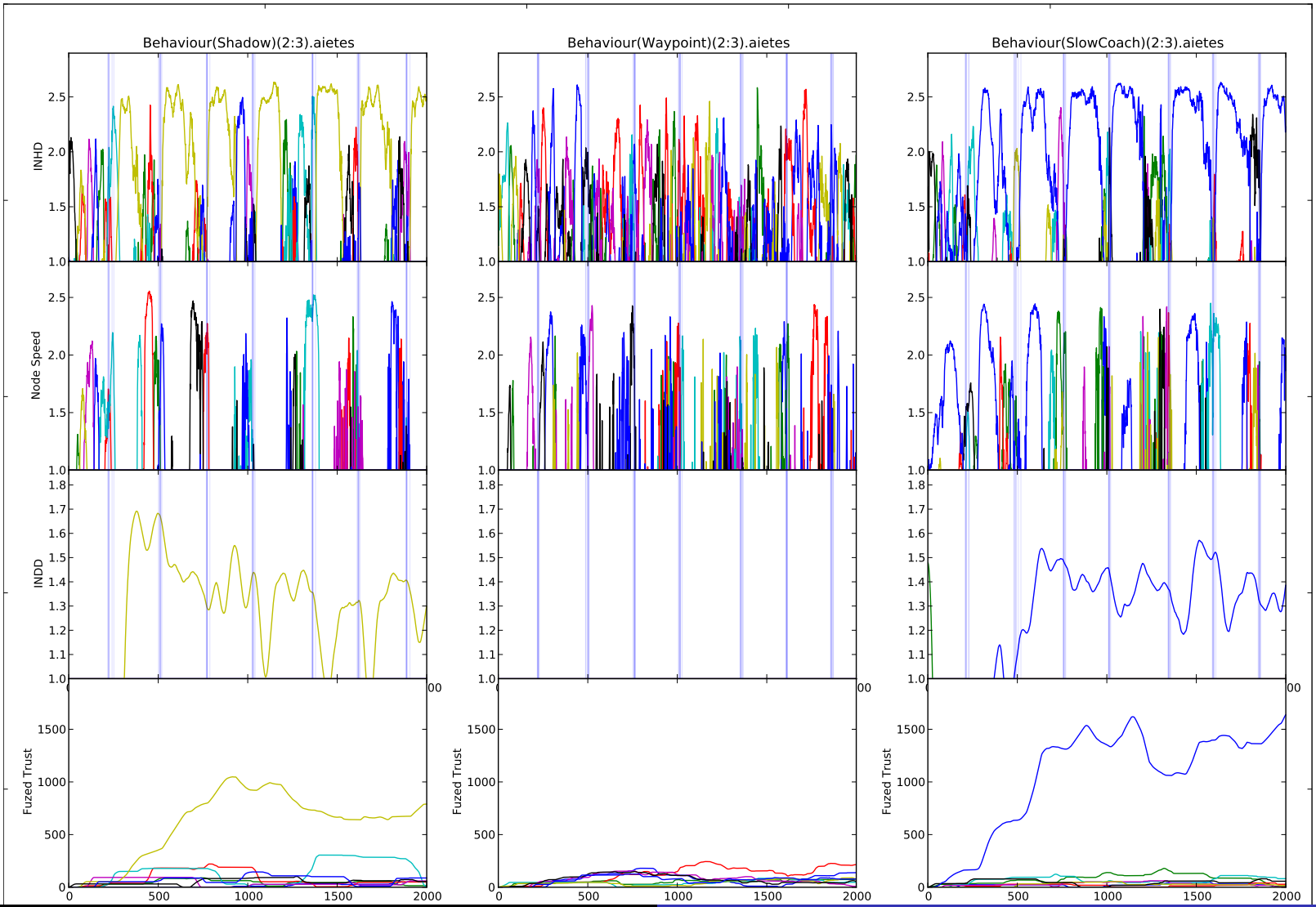
Trust in Mobile Autonomous Underwater Vehicles

- Flocking with Intent: MCM, Port Protection, Survey, Protection Detail, etc.
- Metric Selection in collaboration CMRE/DSTL
  - Inter Node Heading Deviation
  - Inter Node Distance Deviation
  - Node Speed
- Behaviour selection for testing
  - Shadow
  - Slowcoach
  - Spy
  - Sloth

Raw Behavioural Metric Assessment in AUVs



Behavioural Trust Assessment in AUVs



Challenges in Multi-vector Trust

- How to define optimality in trust assessment when dealing with multiple vectors and transitive trust?
- Is there a quantifiable benefit to cross-domain comparison beyond single vector Trust?
- Is there an optimal generic cross-domain comparator?

References

Ji Guo. "Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks". In: (2012).

Huaizhi Li and Mukesh Singhal. "Trust Management in Distributed Systems". In: *Computer (Long. Beach. Calif).* 40.2 (2007), pp. 45–53. ISSN: 00189162. DOI: 10.1109/MC.2007.76. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4085622.

Fengchao Zuo. "Determining Method for Grey Relational Distinguished Coefficient". In: *SIGICE Bull.* 20.3 (Jan. 1995), pp. 22–28. ISSN: 0893-2875. DOI: 10.1145/202081.202086. URL: http://doi.acm.org/10.1145/202081.202086.

The End