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

June 8, 2015

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] **Li2007**.

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]

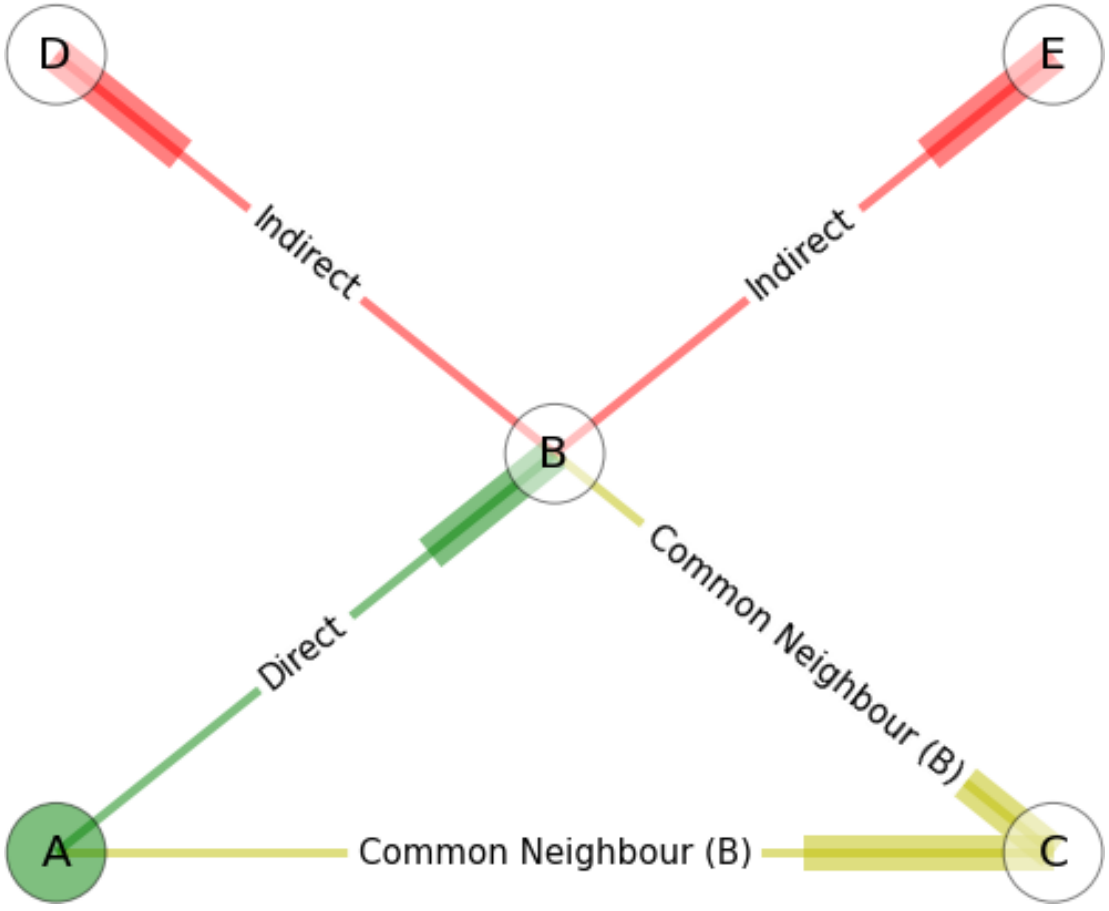
[1] **Li2007**.

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] **Li2007**.

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 [**Guo2012**]