Trust Framework Operation in Autonomous Marine Communications Environments

Andrew Bolster[*] , Alan Marshall, Ji Guo

Advanced Networks Research Group,
Department of Electrical Engineering & Electronics,
University of Liverpool, UK
{andrew.bolster,alan.marshall}@liv.ac.uk
http://www.anrg.liv.ac.uk/

Abstract. As mobile ad-hoc networks (MANETs) grow beyond the terrestrial arena, their operation and the protocols designed around them must be reviewed to assess their suitability and optimality in different communications environments to ensure their continues security, reliability, and performance.
This paper presents an overview of trust assessment within classical adhoc networking environments (Terrestrial MANET), including a critique of previous group work in this area utilitsing Fuzzy Sets and Gray Theory to construct a Trust Management Framework (TMF) for decentralised ad-hoc networks. We then present a comparative study on the operation and performance of such trust frameworks between the terrestrial and underwater communications environments.

Keywords: ad-hoc, MANET, trust, marine, underwater

1 Introduction

Trust Management Frameworks (TMFs) provide information regarding the estimated future states and operations of nodes within networks. They are used to optimize the performance of a system of systems (i.e. collections of autonomous, semi-autonomous, and/or human systems) in the face of malicious, selfish, or defective behavior by one or more nodes within such a system. Previous research has established the advantages of implementing distributed TMFs in terrestrial, 802.11 based mobile ad-hoc networks (MANETs) [Guo et al., 2011]

Trust Management Frameworks (TMFs) provide information regarding the estimated future states and operations of nodes within networks. They are used to optimize the performance of a system of systems (i.e. collections of autonomous, semi-autonomous, and/or human systems) in the face of malicious, selfish, or defective behavior by one or more nodes within such a system. Previous

[*] Please note that the LNCS Editorial assumes that all authors have used the western naming convention, with given names preceding surnames. This determines the structure of the names in the running heads and the author index.

research has established the potential advantages of implementing distributed TMFs in mobile ad-hoc networks (MANETs) [Li and Singhal, 2007]

Current TMFs generally use a single type of observed action to derive trust metrics, e.g. successfully forwarded packets. These historical observations then inform future decisions of individual nodes, for example, the selection of a forward router with the highest previous forwarding success rate [Li et al., 2008].

Recent work has demonstrated the use of a number of metrics together, forming a vector of trust; in the case of [Guo, 2012], metrics related to inter-node communications. This vectorized trust allows a system to detect anomalous behavior and identify the tactics used to undermine or subvert trust.

1.1 Trust in MANETs

In Human trust relationships it can be seen that there can be several perspectives of Trust for example organizational, sociological, interpersonal, psychological and neurological [Lee and See, 2004].

For the purposes of this work we can define two perspectives: Design and Operational. These are summarised as follows:

- Design Trust. When an autonomous system is under development a level of Trust is established in it through the manner in which it has been designed and tested. This is the same as conventional systems. The difference with systems that have high-levels of autonomy is that they are designed to behave adaptively to dynamic environments that are difficult to fully predict prior to operational deployment. For example, in a navigation system it is difficult to predict the dynamic environment it will need to adapt to. So Trust needs to be developed that the design and test of such systems are sufficient to predict that operational solutions will be, if not optimal, at least satisfactory.
- Operational Trust. Effectively, trust that both the individual nodes withing system are operating as expected (which is inevitably tied in with, but distinct from Design Trust); and that the interfaces between the operator and the system are as expected. This latter aspect covers issues such as physical/wireless links and interpretation of data at each end of such a communication link.

In addition to the two perspectives of trust identified, it is necessary to define and classify Operational Trust into two distinct but related sections, which we define as being:

- Hard Trust or technical trust, being the quantative measurement and communication of the expectation of an actor performing a certain task, based on historic performance and through consensus building within a networked system. Can be thought of as a de-risking strategy to measure the ability of a system to perform a task unsupervised.
- Soft Trust or common trust, being the qualitative assessment of the ability of an actor to perform a task or operation consistently and reliably based on

social or experiential factors. This is the natural form of trust and is the main motivational driver for the human-factors trust discussion. Can be rephrased as the level of confidence in an actor to perform a task unsupervised.

It is already clear that these two definitions are extremely close in their construction, but represent fundamentally different approaches to trust, one coming from a sociological perspective of person-to-person and person-to-group relationships from day to day life, and the other coming from a statistical or formal appraisal of an activity by a system.

1.2 Existing Trust Management Frameworks

Recently, various models and algorithms for describing trust and developing trust management in distributed systems, P2P communities or wireless networks have been considered.

- *The Objective Trust Management Framework* takes a Bayesian network approach and introduces the idea of applying a Beta function as an encapsulation method, combining "Trust" and "Confidence of Assessment" into a single value (Li et al. 2008). OTMF however does not appropriately combat multi-node-collusion in the network (Cho, Swarmi and Chen 2011).
- *Trust-based Secure Routing (Moe, Helvik and Knapskog 2008)* demonstrated an extension to Dynamic Source Routing (DSR), incorporating a Hidden Markov Model of the wider ad-hoc network, reducing the efficacy of Byzantine attacks, particularly black-hole attacks but, along with many more TMFs surveyed in (Cho, Swarmi and Chen 2011), falls under the same limitation of focusing on single metric observation.

These single metric TMFs provide malicious actors with a significant advantage if their activity is undetectable by that one assessed metric, especially if the attacker knows the metric in advance. The objective of operating a TMF is to increase the confidence in, and efficiency of, a system by reducing the amount of undetectable negative operations an attacker can perform. This space of potential attacks can be described as the Threat Surface. In the case where the attacker can subvert the TMF, the metric under assessment by that TMF does not cover the threat mounted by the attacker. In turn, this causes a super-linearly negative effect in the efficiency of the network. The TMF is assumed to have reduced the threat surface when in fact it has simply made it more advantageous to attack a different part of it. (Haung, Hong and Gerla 2010) also raised the need for a more expanded view of trust but did so with a domain-partitioning approach rather than combining trust assessments from multiple domains within networks.

Guo ('we'?) demonstrated the ability of Grey Relational Analysis (GRA) to normalize and operationally combine disparate traits of a communications link into a single comparable value, a trust vector (Guo 2012). For applications involving low fidelity, temporally sparse metrics with unknown statistical distributions, GRA is a more stable comparative analysis, providing an interval of potential trust values rather than fuzzy-logic or the Bayesian-Beta distributions found in current TMFs (Liu 2006). It is this work that is being expanded upon in paper.

1.3 Systematic Constraints in Marine Acoustic Networks

In this section, we review selected features of the underwater communications channel, highlighting particular challenges and differentials against terrestrial equivalents.

The key challenges of underwater acoustic communications are centred around the impact of slow and differential propogation of energy (RF, Optical, Acoustic) through water, and it's interfaces with the seabed / air. The resultant challenges include; long delays due to propogation, significant inter-symbol interference and Doppler spreading, fast and slow fading due to environmental effects (aquatic flora/fauna; surface weather), carrier-frequency dependent signal attenuation, multipath caused by the medium interfaces at the surface and seabed, variations in propogation speed due to depth dependant effects (salinity, pressure, gaseous concentrations), and subscequent beam-lensing due to that same propogation variation. This final effect in combination with with the multipath nature of the medium result in supposedly "line of sight" propogations being extremely unreliable for estimating distances to targets, as the first arriving beam has bent in the medium, and commonly has bounced between the surface/seabed before arriving at a receiver.

The attenuation that occurs in an underwater acoustic channel over a distance d for a signal about frequency f in linear and dB forms respectivly is given by

$$A(d,f) = A_0 d^k a(f)^d \tag{1}$$

$$10 \log A(d,f)/A_0 = k \cdot 10 \log d + d \cdot 10 \log a(f) \tag{2}$$

where A_0 is a unit-normalising constant, k is a spreading factor (commonly taken as 1.5), and $a(f)$ is the absorption coefficient, expressed empiracally using Thorp's formula3

$$10 \log a(f) = 0.11 \cdot \frac{f^2}{1+f^2} + 44 \cdot \frac{f^2}{4100+f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \tag{3}$$

1.4 Trust Requirement in Marine Networks

In this section we establish the requirement for communications trust in acoustic marine networks, extending and expanding on the generic assessment given in 1.1

Table 1. Comparison of Base-Simulation constraints as applied between Terrestrial and Marine communications

Parameter	Unit	Terrestrial	Marine
Simulated Duration	s	300	36000
Simulated Area	km^2	0.7	0.7
Transmission Range	km	0.25	1.5
Number of Nodes		6	6
Comms Medium		RF(802.11)	Acoustic(CSMA)
Propogation Speed	m/s	3×10^8	1490
Center Frequency	Hz	2.6×10^9	10^3
Bandwidth	Hz	22×10^6	10^3
Routing Protocol		DSDV	FBR
Mobility		Various	Various
Max Speed	ms^{-1}	5	1.25
Data Rate	bps	10^6	300
Packet Size	bits	4096	9600
Destination Selection		Random	Random
Single Transmission Duration	s	10	32
Single Transmission Size	bits	10^7	9600

2 Previous Work

2.1 Experimental Scenarios

Four Mobility scenarios were used to explore the trust-behaviour, covering the majority of MANET operational requirements;

- All Nodes Static
- Central node performing a random walk with leaf-nodes static
- Leaf-nodes randomly walking with central node static
- All nodes randomly walking

Nodes the six nodes were arranged in the form of a flattened pentagon with the 'central' node places near the geometric middle. This imperfect placement was to ¡make the experiment easier to write with round numbers?¿

3

¡++¿

Acknowledgments. The heading should be treated as a subsubsection heading and should not be assigned a number.

4 The References Section

References

[Guo, 2012] Guo, J. (2012). Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks.

[Guo et al., 2011] Guo, J., Marshall, A., and Zhou, B. (2011). A New Trust Management Framework for Detecting Malicious and Selfish Behaviour for Mobile Ad Hoc Networks. *2011IEEE 10th International Conference on Trust Security and Privacy in Computing and Communications*, pages 142–149.

[Lee and See, 2004] Lee, J. D. and See, K. A. (2004). Trust in automation: designing for appropriate reliance. *Human factors*, 46(1):50–80.

[Li and Singhal, 2007] Li, H. and Singhal, M. (2007). Trust Management in Distributed Systems. *Computer*, 40(2):45–53.

[Li et al., 2008] Li, J., Li, R., and Kato, J. (2008). Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Communications Magazine*, 46(4):108–114.

□ The final LaTeX source files

□ A final PDF file

□ A copyright form, signed by one author on behalf of all of the authors of the paper.

□ A readme giving the name and email address of the corresponding author.