Background on Trust and its Applications to MANETs

Andrew Bolster

October 13, 2015

1 Trust Definitions and Perspectives

For a term that is so common in every-day speech, Trust is a challenging discussion area, particularly given the wealth of proposed definitions (Table 1). Beyond these dry, vague, and often “fuzzy” definitions, there is a significant ontological conflict between the subjective and objective perspectives of trust; is “trust” an attribute of the actor performing a given action, or of the observer of such an action? Or indeed is trust itself an action upon a relationship between actors? Is it qualitative or quantitative? These questions have challenged philosophers, psychologists and social scientists for decades.

More of these in the bookmarks list

In human trust relationships it is recognized that there can be several domains of Trust for example organizational, sociological, interpersonal, psychological and neurological [LS04].

These domains of trust are, from a human perspective, quite natural and are formed during the earliest stages of linguistic integration. This leads to recognisable deviations in the experiential concept of “trust” across cultures with differing linguistic histories. This has led to a wealth of work in the

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 articular action important to the trustor, irrespective of the ability to monitor or control that other party	[MDS95]
An expectancy held by and individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon	[Rot67]

Table 1: Definitions of Trust

social sciences (as well as management schools across the world) in to how to develop, understand, and repair trust across cultural boundaries.[OBMK11]

Get more citations for this paragraph, need background on multicultural definitions rather than second hand

1.1 Modeling of Trust Relationships

Mayer et al [MDS95] proposed a model of trust that encapsulates generalised factors of perceived trustworthiness in interpersonal relationships (Table 2), accommodating a subjective trustworthiness and risk-taking potentiality on the part of the trustor. This formulation of trust allowed a wider discussion of the characteristics of trust relationships, both between individuals and within networks or communities.

Lee and See [LS04] extended and synthesised Mayer et al's approach to personal and interpersonal trust towards a generalised concept of trust for human and autonomic/autonomous systems with the following alternative contextual definitions (including their approximate mappings to Mayer et al's approach

Factor	Definition
Ability	Collection of skills, competencies, capabilities and characteristics that enable a party to have influence or action within some specific domain
Benevolence	The extent to which a trustee is believed to want to do good to or by the trustor beyond a selfish profit motive
Integrity	Acceptance or adherence to a common set of principals of operation that the trustor finds acceptable

Table 2: Factors of Trust[MDS95]

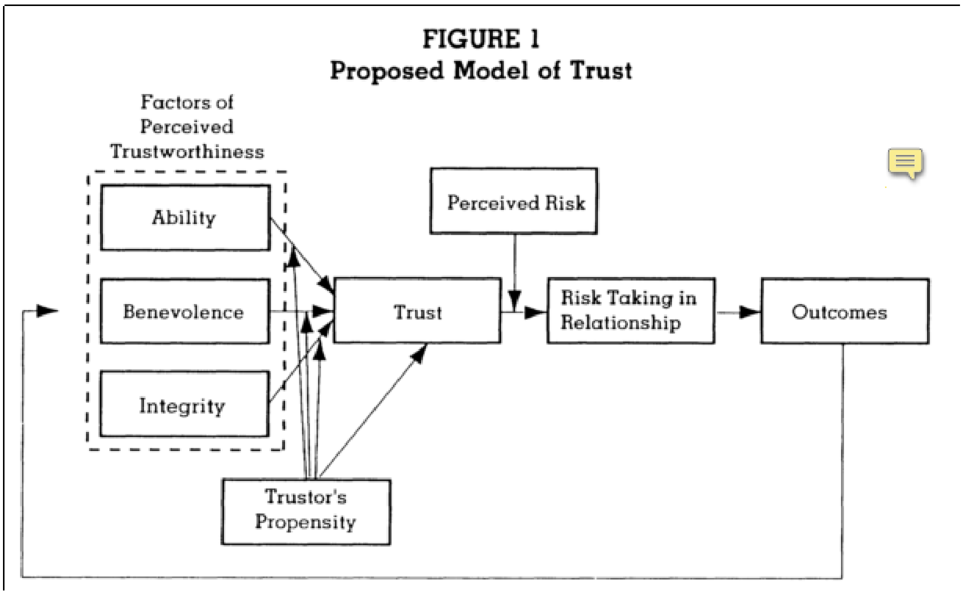

Figure 1: Model of Trust [MDS95]

Factor	Definition	Mayer Term
Performance	‘The current and historical operation of the automation, including characteristics such as reliability, predictability, and ability	Ability
Process	The degree to which the automation’s algorithms are appropriate for the situation and able to achieve the operators goals.	Integrity
Purpose	The degree to which the automation is being used within the realm of the designers intent	Benevolence

Table 3: Factors of Trust for Autonomous Systems[LS04]

1.2 Characteristics of Trust Relationships

There are five commonly considered characteristics or attributes of Trust relationships in general, but not all relationships exhibit them and they are not assumed to be a complete specification of Trust:

- *Multi-Party* - One-to-one; one-to-many; many-to-one; many-to-many. Trust is not an absolute characteristic of a lone individual. Trust may include multi-agent abstractions (one-to-many), such as a preferential trust/distrust towards a group exhibiting a particular attribute, e.g. members of the armed forces / police services. Likewise, there can be trustor/trustee attributes that can generalise relationships between collectives (many-to-many), e.g. Jets and Sharks

if I can get away with citing Sodenheim I’d be very happy

- *Transitive* - Trust assessments can be shared (i.e. recommendations), where this second order trust assessment incorporates both the observed trustworthiness of the trustee, as well as the trustworthiness of the intermediate trustor. In some models this is further extended to include out-of-network intermediate trustors that have some other defined authority, e.g. PKI Certificate Authority

- *Evidential* - Trust must be based on some form of evidence-based observation or assessment, such as historical success rates of performing a certain action, or second-hand observations of trust from a third party.

- *Directional Asymmetry* - The majority of relationships are bi-directional but are asymmetric, i.e. between two entities who "trust" each other, there are two independent trust relationships that may have very different "values" or extents.

- *Contextual* - Trust can be variable and loosely coupled between contexts with respect to the action being assessed or the environment within which the trustee is operating, e.g. Doctors are trusted to perform medical procedures but that trust may not improve their success at correctly wiring an electrical plug. However there are plenty of counter-examples to this, as from [MDS95], two of the three listed factors of trust are "Benevolence" and "Integrity" and are unrelated to the ability of a trustee to perform a particular action, so it is reasonable to make an initial assumption that if a trustee is being benevolent in one activity or context, that that benevolence *should* extend to other contexts.

1.3 Topologies of Trust Networks

Beyond the attributes or characteristics of an individual trust relationship, within any multi party sparsely connected network or community, topological context is useful in both establishing trust and in disseminating observations for collaborative assessment.

Missing figure

Trust Topologies, Direct, Indirect, Recommender, etc. We've done it a dozen times before, may as well make a new graphic

2 Trust in MANETs

2.1 Trust Perspectives in Autonomous Operation

For the purposes of this work we define two perspectives on trust for autonomous systems: Design and Operational. These are summarised in Table 4. It is useful to further define and classify Operational Trust into two distinct but related sections defined in Table 5.

Work out how to reference across chapters in a multi doc

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. For the purposes of this work, we are concerned with the analytical establishment of hard trust within a topologically dynamic network of autonomous actors.

2.2 Levels of Trust

Trust relationships operate as part of a system architecture, and can quite often get confused. Sun[SIHL08] suggests that within these there are two overarching forms of trust:

This section may be superfluous

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. Given that systems that have high-levels of autonomy are designed to behave adaptively to dynamic environments, it is challenging to fully predict such non-deterministic behaviours prior to operational deployment. For example, in a navigation system it is difficult to predict the dynamic environment it will need to adapt to. Trust needs to be developed that the design and test of such systems are sufficient to predict that operation will be, if not optimal, at least satisfactory.
Operational Trust	Trust at runtime or in-situ that both the individual nodes within a system are operating as expected 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. Operational Trust is functionally derived from, but distinct from Design Trust.

Table 4: Trust Perspectives with respect to autonomous systems

Hard Trust or technical trust	The quantitative 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 and monitor the ability of a system, or another actor within a system, to perform a task unsupervised.
Soft Trust or common trust	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 human form of trust and is the main motivational driver for the human-factors trust discussion in *OTHER CHAPTER*. Can be rephrased as the level of confidence an operator has in an actor to perform a task unsupervised.

Table 5: Trust Perspectives within Operational Trust

- Behavioural: That one entity voluntarily depends on another entity in a specific situation
- Intentional: That one entity would be willing to depend on another entity

These concepts closely mirror the previous definitions of Hard and Soft trust respectively, one (Behavioural) being an invested dependency given certain parameters being satisfied, mirroring Hard Trust, and the other (Intentional) being the capacity for belief in another entity, analogous to Soft Trust. It is suggested that these overarching forms are supported by and indeed are drawn from four major constructs within social and networked environments:

- Trusting Belief: the subjective belief within a system that the other trusted components are willing and able to act in each-others best interests

- Dispositional Trust: a general expectation of trustworthiness over time
- Situational Decision Trust: in-situ risk assessment where the benefits of trust outweigh the negative outcomes of trust
- System Trust: the assurance that formal impersonal or procedural structures are in place to ensure successful operation.

Sun argues that only System Trust and Behavioural Trust are relevant to trusted networking applications. However, it is arguable that in any network where the operation of that network is not the only concern, or where that network has to interact with any operator, then all of these factors come into play. Both System and Behavioural trust rely on what Sun calls a Belief Formation Process, or a trust assessment, while the other trust constructs deal with the interactions between trust and decision making against an internal assessment of network trustworthiness.

2.3 Trust Model Design Considerations

Trust is the level of confidence one agent has in another to perform a given action on request or in a certain context. Trust in the autonomous or semi-autonomous realm is the ability of a system to establish and maintain confidence in itself or another systems' operations. Managing this trust can be used to predict and reason on the future interactions between entities in a system, such as an autonomous mobile ad-hoc network (MANET).

The distributed and dynamic nature of MANETs mean that it is difficult to maintain a trusted third party (TTP) or evidence based trust system such as Certificate Authorities or using Public Key Infrastructures (PKI).Therefore, a distributed, collaborative system must be applied to these networks. Such distributed trust management frameworks aim to de-

possibly worthwhile doing more background on the tect, identify, and mitigate the impacts of malicious actors by distributing per-node assessments and opinions to collectively self-police behaviour.

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 to different communications environments, ensuring their continued security, reliability, and performance.

Trust Management Frameworks (TMFs) provide information to assist the estimation of future states and actions of nodes within networks. This information is used to optimize the performance of a network against malicious, selfish, or defective misbehaviour by one or more nodes. Previous research has established the advantages of implementing TMFs in 802.11 based MANETs, particularly in terms of preventing selfish operation in collaborative systems [LS07], and maintaining throughput in the presence of malicious actors [BL02]

There are five topics that are important to address in any MANETs trust model [KSGM03]:

- The trust model should be without infrastructure. Because the network routing infrastructure is formed in an ad-hoc fashion, the trust management can not depend on, e.g., a trusted third party (TTP). There is no public key infrastructure (PKI), where some center nodes monitor the network, and publish illegal nodes periodically. In a MANET, there are no certification authorities (CA) or registration authorities (RA) with elevated privileges etc.

- The trust model should be anonymous because of the anonymity of mobile nodes in MANETs.

- The trust model should be robust. That is, it can be robust to all kinds of unfriendly attacks and the network itself should not be susceptible to attacks by unfriendly nodes. Moreover, in the presence of malicious nodes, they may attempt to subvert the model in order to get the unfairly good trust value.

- The trust model should have minimal control overhead in accordance with computation, storage, and complexity.
- The trust model should be self-organized. MANETs are characterized to have dynamic, random, rapidly changing and multi-hop topologies composed of variably bandwidth-constrained links

3 Current Trust Management Frameworks

Distributed trust management frameworks for MANETs aim to detect, identify, and mitigate the impacts of malicious actors by distributing per-node assessments and opinions to collectively self-police behaviour. Various models and algorithms for describing trust and developing trust management in distributed systems, P2P communities or wireless networks have been considered. Taking some examples;

- *Hermes Trust Establishment Framework* takes a Bayesian Beta function to model per-link Packet Loss Rate (PLR) over time, combining "Trust" and "Confidence of Assessment" into a single value [ZMHT05].
- *The Objective Trust Management Framework* takes a Bayesian approach and introduces the idea of applying a Beta function to changes in the per-link Packet Loss Rate (PLR) over time, combining "Trust" and "Confidence of Assessment" into a single value [LLK$^+$07]. OTMF

however does not appropriately combat multi-node-collusion in the network [CSC11].

- *Trust-based Secure Routing [MHK08]* 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 is limited by focusing on single metric observation (PLR)[CSC11].

- *CONFIDANT*; [BL02] presented an approach using a probabilistic estimation of normal observations, similar to OTMF. They also introduced a greedy topology weighting scheme that internally weighted incoming trust assessments based on historical experience of the reporter.

- *Fuzzy Trust-Based Filtering*; [LLZ+08] presented a method using Fuzzy Inference to cope with imperfect or malicious recommendation based on a probabilistic estimation of performance using conditional similarity to classify performance using overlapping Fuzzy Set Membership functions to collaboratively filter reputations across a network.

- *Multi-parameter Trust Framework for MANETs (MTFM)* uses a number of communications metrics together for form a vector of trust, apply grey information theory to allow a system to detect and identify the tactics being used to undermine or subvert trust[GMZ11]

3.1 Single Metric Trust Frameworks

The Hermes trust establishment framework [ZMHT05] uses Bayesian reasoning to generate a posterior distribution function of “belief”, or trust,

Expand background detail on more frameworks given a sequence of observations of that behaviour, $p(B|O)(1)$.

$$p(B|O) = \frac{p(O|B) \times p(B)}{\rho} \tag{1}$$

Where $p(B)$ is the prior probability density function for the expected normal behaviour, and ρ is a normalising factor. Due to it's flexibility and simplicity, Hermes assumes that $p(B)$ is a Beta function, and therefore the evaluation of this trust assessment is based around the expectation value of the distribution (2) where α and β represent the number of successful and unsuccessful interactions respectively for a particular node i.

A secondary measurement of the confidence factor of the trust assessment t is generated as (3) and these measurements are combined to form a "trustworthiness" value T (4).

$$t_i \to E[\text{beta}(p|\alpha, \beta)] = \frac{\alpha_i}{\alpha_i + \beta_i} \tag{2}$$

$$c_i = 1 - \sqrt{\frac{12\alpha_i\beta_i}{(\alpha_i + \beta_i)^2(\alpha_i + \beta_i + 1)}} \tag{3}$$

$$T_i = 1 - \frac{\sqrt{\frac{(t_i-1)^2}{x^2} + \frac{(c_i-1)^2}{y^2}}}{\sqrt{\frac{1}{x^2} + \frac{1}{y^2}}} \tag{4}$$

In (4), x and y are constants, used weight the two-dimensional polar mapping of trust and confidence assessments (t_i, c_i), and from [ZMHT05], are taken as $x = \sqrt{2}, y = \sqrt{9}$.

Upon this per-node assessment methodology, OTMF overlays an observation distribution protocol so as to make the measurements α_i and β_i representative of the direct and 1-hop networks observations of the target node i, as well as expiring old observations from assessment and eliminating observations from “untrustworthy” nodes.

To date this work has been mostly limited to terrestrial, RF based networks. There are also situations where the observed metrics will include significant noise and occur at irregular, sparse, intervals. Conventional approaches such as probabilistic estimation do not produce trust values that reflect the underlying reality and context of the metrics available, as they require a-priori assumption that the trust value under exploration has an expected distribution, that distribution is mono-modal, and the input metrics are binary. In scenarios with variable, sparse, noisy metrics, estimating the distribution is difficult to accomplish a-priori.

Want at least CONFIDANT and Fuzzy in here for contrast

Hermes, OTMF, CONFIDANT, and Fuzzy Trust-Based Filtering can be generalised as single-value probabilistic estimation, based on a Bayesian idea of taking a binary input state and generating an idealised Beta Distribution (5) of the future states of that input generated through an expectation value based on interactions (6).

$$\text{beta}(p|\alpha,\beta) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}p^{\alpha-1}, \text{ where } 0 \leq p \leq 1; \alpha,\beta > 0 \tag{5}$$

$$E(p) = \frac{\alpha}{\alpha+\beta} \tag{6}$$

Where α and β represent the number of successful and unsuccessful interactions respectively.

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 is aware of the observed 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. 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 as the TMF is assumed to have reduced the possible set of attacks when in fact it has only made it more advantageous to attack a different aspect of the networks operation. An example of such a behaviour would be the case in a TMF focused on PLR where an attacker selectively delays packets going through it, reducing the over all throughput of one or more virtual network routes. Such behaviour would not be detected by the TMF.

3.2 Multi-Metric Trust Frameworks

Given the potential incentives to a selfish attacker and potential threats to trust and fairness in sparse, noisy, and constrained environments, single metric trusts discussed above do not suitably cover the exposed threat surface.A multi-metric approach may be more appropriate to capture and monitor the realities of harsh and sparse communications environments.

Probably best to just send a reference forward to the Marine Comms chapter

MTFM[GMZ11] uses Grey Theory[Zuo95] to perform cohort based normalization of metrics at runtime, providing a “grey relational grade” of trust compared to other observed nodes in that interval for individual metrics, while maintaining the ability to reduce trust values down to a stable assessment range for decision support without requiring every environment entered into to be characterised. This presents a stark difference between the Grey and Probabilistic approaches. Grey assessments are relative in both fairly and unfairly operating networks. All nodes will receive mid-range trust assessments if there are no malicious actors as there is nothing “bad” to compare against, and variations in assessment will be primarily driven by topological and environmental factors. Guo et al. [GMZ11] demonstrated the ability of grey relational analysis (GRA) to normalise and combine disparate traits of a communications link such as instantaneous throughput, received signal strength, etc. into a grey relational coefficient (GRC), or a "trust vector" in this instance.

The grey relational vector is given as

$$\begin{aligned} \theta^t_{k,j} &= \frac{\min_k |a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|}{|a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|} \\ \phi^t_{k,j} &= \frac{\min_k |a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|}{|a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|} \end{aligned} \tag{7}$$

where $a^t_{k,j}$ is the value of an observed metric x_j for a given node k at time t, ρ is a distinguishing coefficient set to 0.5, g and b are respectively the "good" and "bad" reference metric sequences from $\{a^t_{k,j} k = 1, 2 \ldots K\}$, i.e. $g_j = \max_k(a^t_{k,j})$, $b_j = \min_k(a^t_{k,j})$ (where each metric is selected to be monotonically positive for trust assessment, e.g. higher throughput is presumed to be always better).

Weighting can be applied before generating a scalar value (13) allowing the detection and classification of misbehaviours.

$$[\theta^t_k, \phi^t_k] = \left[\sum_{j=0}^{M} h_j \theta^t_{k,j}, \sum_{j=0}^{M} h_j \phi^t_{k,j} \right] \tag{8}$$

Where $H = [h_0 \ldots h_M]$ is a metric weighting vector such that $\sum h_j = 1$, and in unweighted case, $H = [\frac{1}{M}, \frac{1}{M} \cdots \frac{1}{M}]$. θ and ϕ are then scaled to $[0, 1]$ using the mapping $y = 1.5x - 0.5$. To minimise the uncertainties of belonging to either best (g) or worst (b) sequences in (12) the $[\theta, \phi]$ values are reduced into a scalar trust value by $T^t_k = (1 + (\phi^t_k)^2/(\theta^t_k)^2)^{-1}$ [HCG+10]. MTFM combines this GRA with a topology-aware weighting scheme (14) and a fuzzy whitenization model (15).

There are three classes of topological trust relationship used; Direct, Recommendation, and Indirect, repeating those discussed in section 1.3.Where an observing node n_i assesses the trust of another target node, n_j; the Direct relationship is n_i's own observations n_j's behaviour. In the Recommendation case, a node n_k which shares Direct relationships with both n_i and n_j, gives its assessment of n_j to n_i. In the Indirect case, similar to the Recommendation case, the recommender n_k does not have a direct link with the observer n_i but n_k has a Direct link with the target node, n_j. These relationships give node sets, N_R and N_I containing the nodes that have recommendation or indirect, relationships to the observing node respectively.

This is currently half empty

$$\begin{aligned} T_{i,j}^{MTFM} =& \frac{1}{2} \cdot \max_s\{f_s(T_{i,j})\}T_{i,j} \\ &+ \frac{1}{2}\frac{2|N_R|}{2|N_R|+|N_I|}\sum_{n\in N_R}\max_s\{f_s(T_{i,n})\}T_{i,n} \\ &+ \frac{1}{2}\frac{|N_I|}{2|N_R|+|N_I|}\sum_{n\in N_I}\max_s\{f_s(T_{i,n})\}T_{i,n} \end{aligned} \tag{9}$$

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:

$$\begin{aligned} f_1(x) &= -x + 1 \\ f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\ f_3(x) &= x \end{aligned} \tag{10}$$

In the case of the terrestrial communications network used in [GMZ11], the observed metric set $X = x_1, \ldots, x_M$ representing the measurements taken by each node of its neighbours at least interval, is defined as $X =$ [packet loss rate, signal strength, data rate, delay, throughput].

Guo et al. demonstrated that when compared against OTMF and Hermes trust assessment, MTFM provided increased variation in trust assessment over time, providing more information about the nodes' behaviours than packet delivery probability alone can.

4 Grey System Theory and Grey Trust Assessment

4.1 Grey numbers, operators and terminology

Grey numbers are used to represent values where their discrete value is unknown, where that number may take its possible value within an interval of potential values, generally written using the symbol $\oplus$. Taking a and b as the lower and upper bounds of the grey interval respectively, such that $\oplus \in [a, b] | a < b$ The "field" of $\oplus$ is the value space $[a, b]$. There are several classifications of grey numbers based on the relationships between these bounds.

This section largely repeats from MTFM discussion but the maths needs explored somewhere

don't think classification is the right word here

Black and White numbers are the extremes of this classification; such that $\dot{\oplus} \in [-\infty, +\infty]$ and $\mathring{\oplus} \in [x, x] | x \in \mathbb{R}$ or $\oplus(x)$ It is clear that white numbers such as $\mathring{\oplus}$ have a field of zero while black numbers have an infinite field.

Grey numbers may represent partial knowledge about a system or metric, and as such can represent half-open concepts, by only defining a single bound; for example $\underline{\oplus} = \oplus(\underline{x}) \in [x, +\infty]$ and $\overline{\oplus} = \oplus(\overline{x}) \in [-\infty, x]$.

Primary operations within this number system are as follows;

$$\oplus_1 + \oplus_2 \in [a_1 + a_2, b_1 + b_2] \tag{11a}$$

$$-\oplus \in [-b, -a] \tag{11b}$$

$$\oplus_1 - \oplus_2 = \oplus_1 + (-\oplus) \tag{11c}$$

$$\begin{aligned}\oplus_1 \times \oplus_2 \in \; & [\min(a_1a_2, a_1b_2, b_1a_2, b_2a_2), \\ & \max(a_1a_2, a_1b_2, b_1a_2, b_2a_2)]\end{aligned} \tag{11d}$$

$$\oplus^{-1} \in [b^{-1}, a^{-1}] \tag{11e}$$

$$\oplus_1/\oplus_2 = \oplus_1 \times \oplus_2^{-1} \tag{11f}$$

$$\oplus \times k \in [ka, kb] \tag{11g}$$

$$\oplus^k \in [a^k, b^k] \tag{11h}$$

where k is a scalar quantity.

4.2 Whitenisation and the Grey Core

The characterisation of grey numbers is based on the encapsulation of information in a grey system in terms of the grey numbers core ($\hat{\oplus}$) and it's degree of greyness (g°). If the distribution of a grey number field is unknown and continuous, $\hat{\oplus} = \frac{a+b}{2}$.

Non-essential grey numbers are those that can be represented by a white number obtained either through experience or particular method. [LL11] This white hissed value is represented by $\tilde{\oplus}$ or $\oplus(x)$ to represent grey numbers with x as their whitenisation. In some cases depending on the context of application, particular gray numbers may temporarily have no reasonable whitenisation value (for instance, a black number). Such numbers are said to be Essential grey numbers.

4.3 Grey Sequence Buffers and Generators

eqs of sequence buffers and partial derivs

Given a fully populated value space, sequence buffer operations are used to provide abstractions over the dataspace. These abstractions can be *weakening* or *strengthening*. In the weakening case, these operations perform a level of smoothing on the volatility of a given input space, and strengthening buffers serve to highlight and

A powerful tool in grey system theory is the use of grey incidence factors, comparing the "likeness" of one value against a cohort of values. This usefulness applies particularly well in the case of multi-agent trust networks, where the aim is to detect and identify malicious or maladaptive behaviour, rather than an absolute assessment of "trustworthiness".

4.4 Grey Trust

Grey Theory performs cohort based normalization of metrics at runtime. This creates a more stable contextual assessment of trust, providing a "grade" of trust compared to other observed entities in that interval, while maintaining the ability to reduce trust values to a stable assessment range for decision support without requiring every environment entered into to be characterised. Grey assessments are relative in both fairly and unfairly operating cohorts. Entities will receive mid-range trust assessments if there are no malicious actors as there is no-one else "bad" to compare against.

Guo[GMZ11] demonstrated the ability of Grey Relational Analysis (GRA)[Zuo95] to normalise and combine disparate traits of a communications link such as instantaneous throughput, received signal strength, etc. into a Grey Relational Coefficient, or a “trust vector”.

In [GMZ11], the observed metric set $X = x_1, \dots, x_M$ representing the measurements taken by each node of its neighbours at least interval, is defined as $X =$ [packet loss rate, signal strength, data rate, delay, throughput]. The trust vector is given as

$$\begin{aligned} \theta_{k,j}^t &= \frac{\min_k |a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|}{|a_{k,j}^t - g_j^t| + \rho \max_k |a_{k,j}^t - g_j^t|} \\ \phi_{k,j}^t &= \frac{\min_k |a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|}{|a_{k,j}^t - b_j^t| + \rho \max_k |a_{k,j}^t - b_j^t|} \end{aligned} \tag{12}$$

where $a_{k,j}^t$ is the value of a observed metric x_j for a given node k at time t, ρ is a distinguishing coefficient set to 0.5, g and b are respectively the '“good” and “bad” reference metric sequences from $\{a_{k,j}^t k = 1, 2 \dots K\}$, e.g. $g_j = \max_k(a_{k,j}^t)$, $b_j = \min_k(a_{k,j}^t)$ (where each metric is selected to be monotonically positive for trust assessment, e.g. higher throughput is always better).

Weighting can be applied before generating a scalar value which allows the identification and classification of untrustworthy behaviours.

$$[\theta_k^t, \phi_k^t] = \left[\sum_{j=0}^{M} h_j \theta_{k,j}^t, \sum_{j=0}^{M} h_j \phi_{k,j}^t \right] \tag{13}$$

Where $H = [h_0 \dots h_M]$ is a metric weighting vector such that $\sum h_j = 1$, and in the basic case, $H = [\frac{1}{M}, \frac{1}{M} \dots \frac{1}{M}]$ to treat all metrics evenly. θ and ϕ are then scaled to $[0, 1]$ using the mapping $y = 1.5x - 0.5$. The $[\theta, \phi]$ values are reduced into a scalar trust value by $T_k^t = (1 + (\phi_k^t)^2 / (\theta_k^t)^2)^{-1}$. This trust value minimises the uncertainties of belonging to either best (g) or worst (b) sequences in (12).

MTFM combines this GRA with a topology-aware weighting scheme(14) and a fuzzy whitenization model(15). There are three classes of topological trust relationship used; Direct, Recommendation, and Indirect. Where an observing node, n_i, assesses the trust of another, target, node, n_j; the Direct relationship is n_i's own observations n_j's behaviour. In the Recommendation case, a node n_k, which shares Direct relationships with both n_i and n_j, gives its assessment of n_j to n_i. The Indirect case, similar to the Recommendation case, the recommender n_k, does not have a direct link with the observer n_i but n_k has a Direct link with the target node, n_j. These relationships give us node sets, N_R and N_I containing the nodes that have recommendation or indirect, relationships to the observing node respectively.

$$\begin{aligned} T_{i,j}^{MTFM} = \frac{1}{2} \cdot \max_s\{f_s(T_{i,j})\}T_{i,j} + \frac{1}{2}\frac{2|N_R|}{2|N_R|+|N_I|}\sum_{n\in N_R}\max_s\{f_s(T_{i,n})\}T_{i,n} \\ + \frac{1}{2}\frac{|N_I|}{2|N_R|+|N_I|}\sum_{n\in N_I}\max_s\{f_s(T_{i,n})\}T_{i,n} \end{aligned} \tag{14}$$

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:

$$\begin{aligned} f_1(x) &= -x + 1 \\ f_2(x) &= \begin{cases} 2x & \text{if } x \leq 0.5 \\ -2x + 2 & \text{if } x > 0.5 \end{cases} \\ f_3(x) &= x \end{aligned} \tag{15}$$

Grey System Theory, by it's own authors admission, hasn't taken root in it's originally intended area of system modelling [LL11]. However, given it's tentative application to MANET trust, taking a Grey approach on a per metric benefit has qualitative benefits that require investigation; the algebraic approach to uncertainty and the application of "essential and non essential greyness", whiteisation, and particularly grey buffer sequencing allow for the opportunity to generate continuous trust assessments from multiple domains asynchronously.

5 Conclusion

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 to different communications environments to ensure their continued security, reliability, and performance. With demand for smaller, more decentralised MANET systems in a range of domains and applications, as well as a drive towards lower per-unit cost in all areas, TMFs are going to be increasingly applied to resource constrained applications, as the benefits and efficiencies they present are significant. Beyond the constraints of the communications environment, knock on pressures in battery capacity, on-board processing, and locomotion simultaneously present opportunities and incentives for malicious or selfish actors to appear to cooperate while not reciprocating, in order to conserve power for instance. These multiple aspects of potential incentives, trust, and fairness do not directly fall under the scope of single metric trusts discussed above, and this context indicates that a multi-metric approach may be more appropriate. These increasingly decentralised applications present unique threats against trust management [Cai11].

One area of application is the underwater marine environment, where extreme challenges to communications present themselves (propagation delays, frequency dependent attenuation, fast and slow fading, refractive multipath distortion, etc.). In addition to the communications challenges, other considerations such as command and control isolation, as well as power and locomotive limitations, drive towards the use of teams of smaller and cheaper autonomous underwater vehicles (AUVs). In underwater environments, communications is both sparse and noisy. Therefore the observations about the communications processes that are used to generate the trust metrics, occur much less frequently, with much greater error (noise) and delay than is experienced in terrestrial RF MANETS.

As such, the use of trust methods developed in the terrestrial MANET space should be reappraised for application within the underwater context [PGP15].

In the next chapter, the marine communications environment will be studied, as will the current state of the art in the use of autonomy in specifically defence related maritime applications.

References

[BL02] Sonja Buchegger and Jean-Yves Le Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc '02*, pages 226–236. ACM Press, 2002.

[Cai11] Andrea Caiti. Cooperative distributed behaviours of an AUV network for asset protection with communication constraints. *OCEANS, 2011 IEEE-Spain*, 2011.

[CSC11] Jin-hee Cho, Ananthram Swami, and Ing-ray Chen. A survey on trust management for mobile ad hoc networks. *Communications Surveys &amp; Tutorials*, 13(4):562–583, 2011.

[GMZ11] Ji Guo, Alan Marshall, and Bosheng Zhou. A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks. *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011*, pages 142–149, 2011.

[HCG+10] Liang Hong Liang Hong, Wu Chen Wu Chen, Li Gao Li Gao, Guoqing Zhang Guoqing Zhang, and Cai Fu Cai Fu. Grey theory based reputation system for secure neighbor discovery in wireless ad hoc networks. *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, 2, 2010.

[KSGM03] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The Eigentrust algorithm for reputation management in P2P networks. *12th International Conference on World Wide Web (WWW)*, page 640, 2003.

[LL11] Sifeng Liu and Yi Lin. *Grey System Theory and Application.* Number 1. Springer-Verlag Berlin Heidelberg, 2011.

[LLK+07] Jie Li, Ruidong Li, Jien Kato, Jie Li, Peng Liu, and Hsiao-Hwa Chen. Future Trust Management Framework for Mobile Ad Hoc Networks. *IEEE Communications Magazine*, 46(4):108–114, April 2007.

[LLZ+08] Junhai Luo, Xue Liu, Yi Zhang, Danxia Ye, and Zhong Xu.

Fuzzy trust recommendation based on collaborative filtering for mobile ad-hoc networks. *2008 33rd IEEE Conference on Local Computer Networks (LCN)*, pages 305–311, 2008.

[LS04] John D Lee and Katrina A See. Trust in automation: designing for appropriate reliance. *Human factors*, 46(1):50–80, 2004.

[LS07] Huaizhi Li and Mukesh Singhal. Trust Management in Distributed Systems. *Computer*, 40(2):45–53, 2007.

[MDS95] Roger C Mayer, James H Davis, and F David Schoorman. An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20(3):709–734, July 1995.

[MHK08] MEG E G Moe, BE E Helvik, and SJ J Knapskog. TSR: Trust-based secure MANET routing using HMMs. *...symposium on QoS and security for ...*, pages 83–90, 2008.

[OBMK11] Tetsushi Okumura, Jeanne M. Brett, William W. Maddux, and Peter H. Kim. Cultural Differences in the Function and Meaning of Apologies. *International Negotiation*, 16:405–425, 2011.

[PGP15] Surya Pavan, Kumar Gudla, and N Preeti. An Overview of Reputation and Trust in Multi Agent System in Disparate Environments. 5(3):498–504, 2015.

[Rot67] Julian B Rotter. A new scale for the measurement of interpersonal trust1. *Journal of Personality*, 35(4):651–665, 1967.

[SIHL08] Yan Lindsay Sun, Rhode Island, Z Han, and K J R Liu. Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, 46(2):112–119, 2008.

[ZMHT05] Charikleia Zouridaki, Brian L Mark, Marek Hejmo, and Roshan K Thomas. A quantitative trust establishment framework for reliable data packet delivery in MANETs. *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 1–10, 2005.

[Zuo95] Fengchao Zuo. Determining Method for Grey Relational Distinguished Coefficient. *SIGICE Bull.*, 20(3):22–28, January 1995.