Multi-domain Grey Trust with Sparse, Asynchronous, Metric Vectors

DRAFT for 8pg submission to TrustCom 15 - 31 March

Andrew Bolster
Department of Electical Engineering and Electronics
University of Liverpool
Liverpool, UK
Email: bolster@liv.ac.uk

Alan Marshall
Department of Electical Engineering and Electronics
University of Liverpool
Liverpool, UK
Email: alan.marshall@liv.ac.uk

***Abstract*—This paper presents a methodology for establishing continuous trust based on sparse and asynchronous trust metric observations across multiple domains of measurement. Using Grey Sequence Buffer Operations and Grey Generator Filters, we show that by performing per-domain filtering**

is there a better phrase for 'filling in the gaps'

while performing cross-domain vector whitenization, a more stable and practical trust assessment is produced.

We test this methodology within the context of an Underwater Autonomous Network.

I. Introduction

Many trust systems operate on the basis of establishing closed system models based on noisy or perturbed information inputs, sourced by decentralised agents or nodes, with an aim to collaboratively establishing additional information about the expected states and behaviours of other agents within a system.

Need to say somewhere that 'agent' and 'node' are used interchangeably in this document

As such, trust systems can be described as fundamentally uncertain, particularly in the areas or reputation establishment and trust chaining.[**?**]. Adding to this state the highly dynamic features of many aspects of trust theory applications (Ad Hoc Networks, Online Markets, etc.), we can generalise the sources of incomplete information from a single nodes perspective as being part of 4 cases.

- Information on the system's boundary is incomplete
- Information about the range of system behaviours is incomplete
- Information about the structure of the system is incomplete or out of date
- Information about observed parameters (metrics) is incomplete or out of date.

These cases of incompleteness of information are closely mirrored by those for which grey theory was originally posited as a form of system modeling, putting information incompleteness at the centre of the assessment. While some work [1] has been done to apply grey theory to a trust context, it has not been fully explored. Guo applies grey analysis to generate a "trust vector" from the grey whitenisation of independent or near-independent metrics. In this paper we demonstrate a methodology that applies Grey Sequence operations and Grey Generators (conceptually analogous to Sequential Bayesian Filtering") to provide continuous trust assessment in a sparse, asynchronous metric space across multiple domains of trust.

II. Trust as an incomplete system characteristic

While application specific trust management frameworks are often based on a very limited space of available metrics, the problem of establishing trust in dynamical systems such as social, economic or autonomous systems have the opportunity to tap in to a wide range of potential metric spaces. Taking the example of Mobile Ad-Hoc Networks (MANET), the variable most applied to the assessment of trust is the packet error rate, or more generally, the number of successful and unsuccessful interactions between two agents within a system. However, a wealth of other information is available within this example; for instance the delay in communications from one node to another; the total throughput of particular network links; and in the case of wireless networks, the strength of received signals. Looking beyond the communications domain, within such a MANET, information is also usually available regarding the physical domain of a network; the relative positioning and motions of nodes within a network can also be used to inform the generation of trust assessments.

III. Grey System Theory

A. 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.

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;

$$\oplus_1 + \oplus_2 \in [a_1 + a_2, b_1 + b_2] \tag{1a}$$
$$-\oplus \in [-b, -a] \tag{1b}$$
$$\oplus_1 - \oplus_2 = \oplus_1 + (-\oplus) \tag{1c}$$
$$\oplus_1 \times \oplus_2 \in [\min(a_1a_2, a_1b_2, b_1a_2, b_2a_2), \max(a_1a_2, a_1b_2, b_1a_2, b_2a_2)] \tag{1d}$$
$$\oplus^{-1} \in [b^{-1}, a^{-1}] \tag{1e}$$
$$\oplus_1 / \oplus_2 = \oplus_1 \times \oplus_2^{-1} \tag{1f}$$
$$\oplus \times k \in [ka, kb] \tag{1g}$$
$$\oplus^k \in [a^k, b^k] \tag{1h}$$

where k is a scalar quantity.

B. 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. [2] 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.

C. 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".

D. 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 nodes in that interval, 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. Grey assessments are relative in both fairly and unfairly operating networks. Nodes will receive mid-range trust assessments if there are no malicious actors as there is no-one else "bad" to compare against.

Guo[1] demonstrated the ability of Grey Relational Analysis (GRA)[3] 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 the case of the terrestrial communications network used in [1], 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]. The trust vector is given as

$$\theta^t_{k,j} = \frac{\min_k |a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|}{|a^t_{k,j} - g^t_j| + \rho \max_k |a^t_{k,j} - g^t_j|} \tag{2}$$
$$\phi^t_{k,j} = \frac{\min_k |a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|}{|a^t_{k,j} - b^t_j| + \rho \max_k |a^t_{k,j} - b^t_j|}$$

where $a^t_{k,j}$ 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 $\{a^t_{k,j} k = 1, 2 \ldots K\}$, e.g. $g_j = \max_k(a^t_{k,j})$, $b_j = \min_k(a^t_{k,j})$ (where each metric is selected to be monotonically positive for trust assessment, e.g. higher throughput is always better).

E. PROSE: Whats the point

Grey System Theory, by it's own authors admission, hasn't taken root in it's originally intended area of system modelling [**?**]. 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;

For a given metric set X such that $X = x_1, \ldots, x_M$ representing the M different types of measurement generated by an observer. If these metrics are not synchronised, for instance if they are interrupt driven such as communications-based observations, generating more abstract measurements requires inherent assumptions about "how to accumulate the data while you wait". For instance, in [**?**], we demonstrated a periodic trust assessment framework for autonomous marine environments, in such an environment, to establish useful, generalised, data, it was necessary to wait for a relatively long time to accumulate enough data to make assessments. However, this left many 'smells'; data was being left in-buffer for a long time before being used to make decisions, and by

the time the data was collated and processed, it could be wildly different from the reality. Further, while some periods could be extremely sparse or even empty, others could be extremely busy with many records having to be averaged down to provide a 'single period' response. Therefore, the implementation of a suitable sequence buffer version of the framework would be beneficial.

Such a sequence buffer framework would involve a tracking predictor that would provide best-guess estimates of an interpolated value for a metric between value updates, and a back-propagation algorithm to retroactively update historical assessments of that metrics so as to better inform any abstracted trust value predictor.

I had initially thought that such a back-propogator would be a total mess as I'd imagined that significant-model-breaking would potetially indicate untrustworthy behaviour, but this is stupid since the per-metric-model has the least information of anyone and is simply there to provide better intermediate values and has no / limited direct impact on the overall trust behaviour.

This backpropogation will probably be a pain to implement as it'd require a retroactive reassessment of trust and could get really messy if it was interrupt driven, but it's better not to prematurly optimise.

IV. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] J. Guo, A. Marshall, and B. Zhou, "A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks," *Proc. 10th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2011, 8th IEEE Int. Conf. Embed. Softw. Syst. ICESS 2011, 6th Int. Conf. FCST 2011*, pp. 142–149, 2011. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6120813

[2] S. Liu and Y. Lin, *Grey System Theory and Application*. Springer-Verlag Berlin Heidelberg, 2011, no. 1. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6044018$\backslash$nhttp://www.springer.com/physics/complexity/book/978-3-642-16157-5

[3] F. Zuo, "Determining Method for Grey Relational Distinguished Coefficient," *SIGICE Bull.*, vol. 20, no. 3, pp. 22–28, Jan. 1995. [Online]. Available: http://doi.acm.org/10.1145/202081.202086