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 System Theory, Sequence Buffer operations and 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

This demo file is intended to serve as a "starter file" for IEEE conference papers produced under LaTeX using IEEEtran.cls version 1.7 and later. I wish you the best of success.

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Trust in Networks

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 $\overset{\bullet}{\oplus} \in [-\infty, +\infty]$ and $\overset{\circ}{\oplus} \in [x,x] | x \in \mathbb{R}$ or $\oplus(x)$ It is clear that white numbers such as $\overset{\circ}{\oplus}$ 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. 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)[2] 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

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

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 $\{a^t_{k,j} k = 1, 2 \dots K\}$, 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).

C. 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 qualatative benefits that require investigation; the algebraic approach to uncertainty and the application of "essential and non essential greyness", whitenization, 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 $X = x_1, \dots, x_M$ 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 inherant 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 implemenation 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-propogation 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] 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