A Multi-Vector Trust Framework for Autonomous Systems

Andrew B. Bolster and **Alan Marshall**
University of Liverpool
{andrew.bolster,alan.marshall}@liv.ac.uk

Abstract

This paper presents an overview of trust assessment schemes for networks of mobile autonomous systems, and proposes a new framework that applies Grey Relational Analysis (GRA) to multiple measurements across multiple types of observations as opposed to current approaches that employ a single metric to derive their trust. This multi-vector approach reveals tactical and strategic information about abnormal, and potentially malicious, behaviors.

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 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.

This paper extends this concept and presents a new multi-vector trust framework that exposes higher-order information such as the subversive strategy employed by selfish/malicious nodes in a network.

Existing Trust Management Frameworks

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.

Multi-vector Trust

Guo demonstrated the ability of Grey Relational Analysis (GRA) to normalize and operationally combine disparate traits of a domain (communications) 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).

The fundamental operation of GRA is the generation of a per-metric Grey Relational Coefficient (GRC) (Zuo 1995), which allows different types of metrics to be compared as part of a vector analysis, presenting the trustworthiness of an operation against the 'best observed' behavior.

We extend this methodology to an N-dimensional trust matrix, combining per-metric and per-domain coefficient analysis. This allows the assessment of information about the tactics of attack, as well as the ability to detect and identify cross-domain and multi-node collusion strategies.

Challenges for implementing Multi-vector trust

The creation of a true multi-vector trust framework first requires investigation into the optimal cross-correlation strategies across multiple domains. In addition, the benefits of generic cross-domain metric comparison need to be determined. For the sake of discussion, it is assumed that the Per-domain GRC's are input directly into a secondary, GRA cycle, that produces a cross-domain GRC interval to indicate the overall system-trust.

Application to Autonomous Underwater Vehicles

One application of this framework is to assess the trustworthiness in networks of autonomous vehicles. In such systems, the physical movement and inter-node communications can be identified as two domains of trust that are appropriate for this cross-domain analysis. Applying stochastic physical metrics can produce a GRC vector for the physical domain (deviations of heading, speed, inter-node spacing, etc.). Taking this with a similar metric set (packet loss rate, signal strength, data rate, delay, throughput, etc.) in the communicative domain presents two vectors of Grey Trust, which have a GRC vector between them. This will enable both existing detection techniques already stated but also the detection of malicious cross-domain behaviors.

Multi-vector trust also helps reduce false positive responses. For example, packet error rate increasing with distance between nodes is a natural process rather than a malicious behavior, which would potentially have alarmed a single-metric or even single-vector TMF.

In an effort to explore the idea of multi-vector trust, we use the example of harbor patrol using sparsely connected Autonomous Underwater Vehicles. In this scenario, nodes are required to distribute themselves across a protected area, but there are not enough nodes to give complete coverage, requiring nodes to patrol to provide necessary coverage.

An example of a malicious behavior in this scenario is for a node to maintain a static position but otherwise perform normally, selfishly preserving its power. Another would be for a node to remain at the rear of the patrol (to keep itself out of danger) but to maintain communications with the edges of the patrol to keep up the appearance of normal operation.

To measure the 'fairness of operation' with respect to energy usage, deviations against average neighbor speed, heading, and spacing are used. Deviations from trustworthy behavior are detected by taking a windowed, weighted, time series of the GRC's of both these metrics and the relevant communications metrics.

Conclusion

In this paper, we proposed multi-vector trust as a model for trust derivation that increases operational safety and efficiency by providing information on both the tactics and strategy of one or more misbehaving or malicious actors in a network.

Acknowledgements

The authors would like to thank MOD/DSTL for sponsoring and assisting in the research.

References

H. Li and M. Singhal, "Trust Management in Distributed Systems," *Computer (Long. Beach. Calif).*, vol. 40, no. 2, pp. 45–53, 2007.

J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 108–114, Apr. 2008.J. Guo, "Trust and Misbehaviour Detection Strategies for Mobile Ad hoc Networks," 2012.

R. Li, J. Li, P. Liu, and H.-H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," *Veh. Technol. Conf.*, pp. 56–60, Apr. 2007.

J. Cho, A. Swami, and I. Chen, "A survey on trust management for mobile ad hoc networks," *Commun. Surv. & Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

M. Moe, B. Helvik, and S. Knapskog, "TSR: Trust-based secure MANET routing using HMMs," *... Symp. QoS Secur. ...*, pp. 83–90, 2008.

D. Huang, X. Hong, and M. Gerla, "Situation-aware trust architecture for vehicular networks," *Commun. Mag. IEEE*, no. November, pp. 128–135, 2010.

K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 305–317, 2006.

F. Zuo, "Determining Method for Grey Relational Distinguished Coefficient," *SIGICE Bull.*, vol. 20, no. 3, pp. 22–28, Jan. 1995.

$$\left[\theta_{k,j}, \varphi_{k,j}\right]^t = \left[\frac{\min_k \left|a_{kj}^t - g_j^t\right| + \rho \max_k \left|a_{kj}^t - g_j^t\right|}{\max_k \left|a_{kj}^t - g_j^t\right|}, \frac{\min_k \left|a_{kj}^t - b_j^t\right| + \rho \max_k \left|a_{kj}^t - b_j^t\right|}{\max_k \left|a_{kj}^t - b_j^t\right|}\right] \ldots \text{(i)}$$

Equation i: Finding the GRC of an action (i.e. metric) j by node k, where g and b are the 'best' and 'worst' values of j in the sample respectively. θ and φ together form a Grey interval for action j by node k at time t

$$GRC(A_k) = [\theta_k, \varphi_k]^t = \sum_{j=1}^{m} h_j \left[\theta_{k,j}, \varphi_{k,j}\right]^t \ldots (ii)$$

Equation ii: Taking the GRC as a weighted sum of samples (metrics) provides a per-node Grey Interval Trust Value for the metric-set A_k (domain)

$$T_k^t = {}^{1}\Big/_{1 + \left(\frac{(\varphi_k^t)^2}{(\theta_k^t)^2}\right)} \ldots (iii)$$

Equation iii: Production of a scalar trust value from a Grey Interval Trust

$$\mathrm{A_{phys}} = \{\text{heading, velocity, internode spacing}\} \ \ldots \text{(iv)}$$
$$\mathrm{A_{comms}} = \{\ \text{PER, RSSI, data rate, delay, throughput}\} \ldots \text{(v)}$$

Equations iv/v: Exemplar metric vectors for the physical (iv) and communications (v) domains

$$[\theta_k, \varphi_k]_{MV}^t = \mathrm{GRC}\left(\left[\mathrm{GRC}(\mathrm{A_{phys}}), \mathrm{GRC}(\mathrm{A_{comms}})\right]\right) \ldots \text{(vi)}$$

Equation vi: Potential simple combination technique across domains

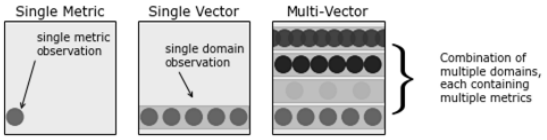

Figure 1 Additional metrics within and across domains provide increased coverage of the potential attack space