

Applying Clustering to a Framework for Generating Trust

Javesh Boodnah and Eric M. Scharf
Queen Mary, University of London
{javesh.boodnah; e.m.scharf}@elec.qmul.ac.uk

Abstract

This paper addresses the issue of trust within the ad hoc context. Several models which claim to model trust are evaluated and a trust framework is then devised which bases itself on clustering technology. Our model aims at providing trust information about originally unknown nodes while making optimum use of computational capacity, which can be quite scarce in pure ad hoc networks. The use of trust data to generate relationships between nodes is therefore strongly favoured to applied cryptography, which generally involves intensive resource consumption. The method proposed also draws on statistical derivations to propose a condition of normality while attempting to provide definition to behaviour.

1. Introduction

Trust as a concept is vague by its very nature. Attempts at its formalisation have been made [Mar94] but it still remains an elusive concept unless properly defined. For the purpose of this paper, we shall stick to the definition that trust is the general belief in an entity to produce a favourable outcome. This is fairly similar to the well-known concept of probability. Currently, there are various types of trust models in place in different areas of computing. While some of these are an integral part of a larger generalised structure with wider areas of application, a few exist as pure trust models in their own right. The main drivers behind the existence of models such as the latter are mainly concerns over security in large distributed systems where it has become important to check the veracity of users' identities. Current relevant areas of research include but are not limited to privacy issues in e-commerce where websites need to strive to protect their customers, leading to the development of certificates for public key encryption. A

branch of Multi Agent Systems is also aimed at automating transactions by examining the issue of trust in the form of reputation systems. Such models attempt to remove the bad agents from the good within an already established community. Other more obvious areas where trust models are adopted are auction sites, such as eBay, which provide a rating system for buyers and sellers such that it then becomes possible for dishonest users to be identified.

However, one of the most pertinent areas where trust issues are now gaining more focus than ever before is that of ad hoc networks, which are essentially peer-to-peer systems operating on a fully decentralised basis. This means that all nodes inside the network are completely autonomous and transactions between them do not rely on a central authority. Therefore the mere consequent potential for uncontrolled rogue nodes in such networks fully justifies the need for the design of a trust framework, capable of ensuring some form of robustness against malicious intent, while at the same time being able to perform reasonably well within the constraints of time and computational capacity.

The rest of this paper is organised as follows: Section 2 analyses selected relevant research and section 3 defines the general requirements for our trust framework. Section 4 elaborates on the proposed model and provides an outlook on future work while section 5 concludes this paper.

2. Existing Trust Models

As defined previously, trust is a belief in an entity for a positive outcome. Of all the trusts models reviewed, some had a two-way formalisation (either complete trust or distrust) while

others had a spectrum of trust values associated with the model. For the latter, that spectrum consisted either of discrete levels of trust or continuous values ranging from 0 to 1.

One interesting feature however was that most of those models defined trust as subjective. Only three associated it to an objective connotation. These are detailed below:

IST's [SJ93] objective model is quite strong as it can be based on observable facts. An agent's trustworthiness is measured by taking into account what the contributions of that agent are. This is seen as 'fact' which is then seen as whether true or false. When the history of such records is kept over a certain period of time, a consistent and dependable trust value can be inferred, provided the observer remains the same. This is subject to how the observed fields are defined, i.e. the more concrete the observed facts are (e.g. "there is chair under the table") then the more reliable the trust values. This is also a useful way for the system to establish a certain level of normality, particularly when trying to establish trust from a generally unknown network.

Chimaera's [TH92] trust model is based on a directed graph of certification authorities (CAs) and weighted certification paths. Neighbouring CAs propagate the trust values and these are used generally at 'face value'. This introduces a certain level of uncertainty within the scheme as the meaning of such values is unclear. Furthermore, since the values are propagated freely, the source that originally defined that value is not always known and hence there is no real way to confirm whether that value is meaningful or if it can be relied upon. Despite highlighting these concerns in the paper, the authors did not follow up on them. A possible solution would have been to attach characteristics of the CAs (like the trust between them and their neighbours) to the propagated trust value. Such a scheme would then allow remote CAs to evaluate the real meaning of the propagated trust value.

Finally, Poblano's [CY01] model is similar to Chimaera's in that trust values

are taken at face value. The difference is that the source of trust values in Poblano is known. In a trust propagation chain the trust value of a node is the opinion of the node prior to it. However whether the source of the trust value is known or not has little impact on the trust model because of the fact that the values are taken at face value with no added information. It is interesting to note that in the case of Poblano, although the trust values are subjective opinions (derived from individual agents), these automatically become objective 'properties' of the agents being trusted as soon as they are propagated to other agents.

The framework being proposed for the ad hoc network is inspired from Chimaera and IST. Distributed temporary authorities, termed Cluster Heads (CHs) are used throughout the network as local concentration points where trust information is collected and evaluated. The IST input stems from the fact that observables, which we call behaviour, are used to be able to infer trust values and maintain (either increase or decrease) such values via the use of databases which will be stored centrally on the CH. A schematic of the framework is proposed in Figure 1.

3. The Framework Requirements

There is a need for the system to be able to model "normality" and to a certain extent (probabilistic) be able to recognise abnormality or anomalies, whether in the form of attacks or genuine network disruptions/outages (physical). This is particularly important in new networks, where no a priori information is available on participating agents or nodes, as is normally the case in "pure" ad hoc networks.

With the CH approach, there is the possibility to correlate information from many monitoring nodes to constantly evaluate the state of the network and therefore initiate responses in real time.

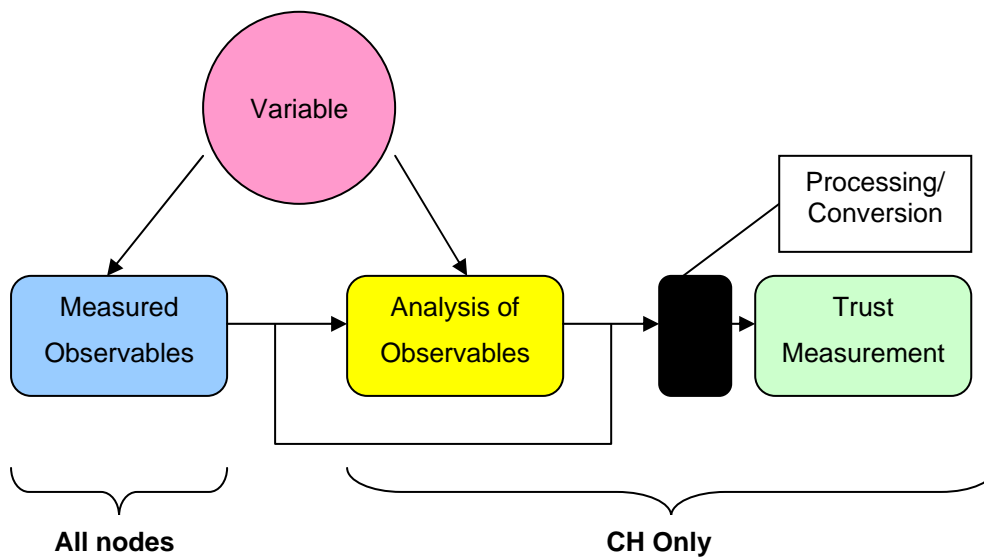


Figure 1. Overview of trust framework (black-box)

We propose 2 layers of detection:

1. At node and CH level – both involve data collection and sorting
2. At CH level – Analysis of the data and translating such data to objective observed behaviour. (Local policies involved in such generation are unique throughout the network, unlike the Chimaera method).

On a practical level, this involves having different kinds of detectors on a distributed scale (geographically) and using different kinds of algorithms (see Figure 2). Whenever events occur, these are then passed to the correlating agent. Such data will include the type of event (whether it's an attack or a genuine outage), the level of anomaly (deviation) and the time stamp.

This can involve quite a lot of computation and the need for non-negligible hardware to store resulting data. This is not always possible in ad hoc networks, depending on the scenario. Hence, there is a strong need to make the behaviour monitoring process as lean as possible, and using the least amount of computation (hence simpler algorithms and simpler statistical estimators) without having a noticeable impact on the accuracy of the detection.

A number of observables (variables) can be defined at this stage from which it is possible to extract some form of trust value for a particular node based on the evaluation it receives from neighbours. Some of these include but are not restricted to the following:

- Network data such as packet sourcing, delivery and transmission, bandwidth utilisation, node latency.
- Physical data such as battery consumption, range and frequency of transmission, determining whether some nodes remain in listening mode (uncooperative behaviour).

Further information on the technicalities of the CH approach can be found in [BS04].

It follows that the crucial link in this whole procedure is the translation that occurs from mapping observed values to the derivation of trust values. Simplified probability equations can provide an overview. However, being able to define and formalise behaviour as a concept is the main challenge and is the focus of current work that goes beyond the scope of this paper.

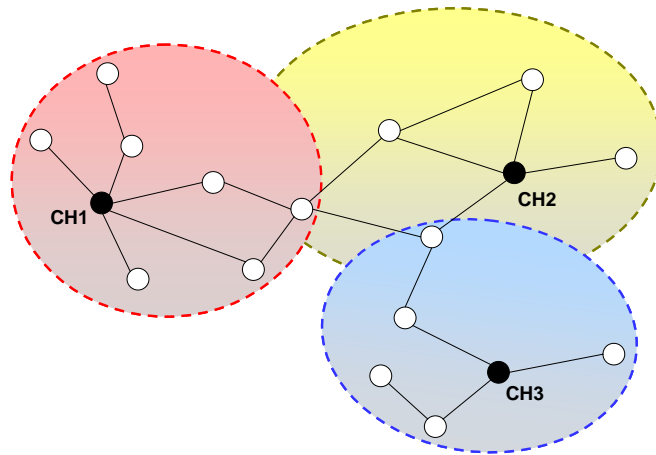


Figure 2. CH approach to trust generation [BS04]

4. Applying the model

The collection of observed data via nodes and CHs is computationally intensive and also adds load onto the already slim resources of the ad hoc environment. Hence, it is imperative to choose the data that is most relevant to trust information and apply it to deduce behaviour. The following implementation based on Kwitt's work [Kwi04] attempts at defining normality so a comparison can be generated.

Traffic monitoring (packet-based)

While monitoring traffic, we observe certain parameters (our observables/variables) and estimate the parameters of their underlying distribution.

Let a random variable X indicate whether a parameter (such as a successful packet transmission at a node) takes on a certain value (denoted by event A , $p = P(A)$) or not. This simulates a Bernoulli experiment since we only have two outcomes.

Thus it follows that

$$\begin{aligned} X(w) &= 1 \text{ if } w \in A \\ &= 0 \text{ if } w \text{ is not } \in A \end{aligned} \quad (4.1)$$

We repeat the same basic random experiment n times. Let another random variable Y indicate the number of successes:

$$Y = \#\{i : X_i = 1, i = 1, \dots, n\}.$$

We get

$$Y = \sum_{i=1}^n X_i \rightarrow Y \approx Bn, p \quad (4.2)$$

The combined probability function of Y_1, \dots, Y_n , is given by the multinomial distribution.

$$Z \approx Mn_{n, p_1, \dots, p_n} \quad (4.3)$$

By assuming that we have enough anomaly-free training traffic, it is possible to estimate the values of the parameter specific multinomial distribution. This can be called the nominal profile.

A packet window of the last N packets, which is shifted one position per new packet arrival is also defined.

Parameters' estimation of the window specific multinomial distribution leads to a current traffic profile.

The maximum likelihood estimator π_i for the probabilities of a multinomial distribution is

$\pi_i = n_i/n$ where n_i denotes the number of occurrences of element i .

We can now calculate the deviation of the current parameters from the expected parameters for normal traffic.

$$d_i = \pi_i \text{ nominal} - \pi_i \text{ current} \quad (4.4)$$

This then constitutes a learning mechanism upon which we can deduce what normality entails. As a guideline, it is safe to estimate that if d_i does not oscillate a consequent amount over different traffic profiles, then the system can be assumed to be behaving normally.

Future Outlook

Once normality is reached, then as long as it is maintained, a given trust value can be inferred by the CH from data provided by neighbouring nodes according to how the trustee is behaving. Furthermore, anomalies or breaches in the trust can then be calculated. How accurate the method proves is probably too hard to estimate at this stage. However, as long as the two criteria below are met:

- Identify anomalies as soon as possible, with the least number of false positives/negatives.
- Make sure the system stays in the anomalous state for the least amount of time as possible.

the method can effectively be considered to be successful. Dynamic trust generation and anomaly detection and elimination based on trust are currently the subject of ongoing investigation and feature as future work.

5. Conclusion

We have looked at a proposed method for trust to be implemented within an ad hoc network. While the model is still being evaluated for added functionality and also being implemented to verify whether it performs as was the aim, this proposal nevertheless defines the reasoning behind proposing such an architecture. It is generally believed that by combining trust with security, it is possible, in most non-sensitive cases to achieve reasonable network stability and safety (in terms of secure communication) without having recourse to intrusive and bulky cryptography which would rapidly consume the resources of a pure ad hoc network, thereby hindering other crucial operative functions such as packet broadcasting and routing.

References

- [BS04] Javesh Boodnah and Eric Scharf. Trust in Ad Hoc Networks: A Novel Approach based on Clustering. In *Proceedings of the London Communications Symposium*, pp. 257-260, 2004.
- [CY01] Rita Chen and William Yeager. Poblano: A distributed trust model for peer-to-peer networks. Technical report, Sun Microsystems, August 2001. www.jxta.org/docs/trust.pdf.
- [Kwi04] Roland Kwitt. A Statistical Anomaly Detection Approach for Detecting Network Attacks. In *6QM Workshop*, 2004.
- [Mar94] Stephen Marsh. *Formalising Trust as a Computational Concept*. PhD thesis, Department of Computing Science and Mathematics, University of Sterling, 1994.
- [SJ93] Nematollaah Shiri and Hasan M. Jamil. Uncertainty as a function of expertise. In *Workshop on Incompleteness and Uncertainty in Information Systems*, 1993.
- [TH92] Anas Tarah and Christian Huitema. Associating metrics to certification paths. In *European Symposium on Research in Computer Science (ESORICS)*, 1992.