On the asymptotic behaviour of formal logic based trust models [1]

V. Liagkou[1,2], E. Makri[4], P. Spirakis[1,2], Y.C. Stamatiou[2,3]

[1]University of Patras, Department of computer Engineering,
26500, Rio, Patras, Greece
[2]Research and Academic Computer Technology Institute, N. Kazantzaki,
University of Patras, 26500, Rio, Patras, Greece
[3]Mathematics Department, 451 10, Ioannina, Greece
[4]University of the Aegean, Department of Mathematics,
83000, Karlovassi, Samos, Greece.
e-mails: liagkou@cti.gr, effiem@aegean.gr, spirakis@cti.gr, istamat@cc.uoi.gr

Abstract

The concept of *trust* plays an important role in the operation and public acceptance of today's computing environment. Although it is a difficult concept to formalize and handle, many efforts have been made towards a clear definition of trust and the development of systematic ways for trust management. Our central viewpoint is that trust cannot be defined, anymore, as consisting of a static set of rules that define systems properties that hold eternally due to the highly dynamic nature of today's computing systems (e.g. wireless networks, ad-hoc networks, virtual communities and digital territories etc.). Our approach is an effort to define trust in terms of properties that hold with some limiting probability as the the system grows and try to establish conditions that ensure that ‘‘good’’ properties hold *almost certainly*. Based on this viewpoint, in this paper we provide a new framework for defining trust through formally definable properties that hold, almost certainly, in the limit in randomly growing combinatorial structures that model ‘‘boundless’’ computing systems (e.g. ad-hoc networks), drawing on results that establish the threshold behavior of predicates written in the first and second order logic. We will also see that, interestingly, some trust models have properties that do not have limiting probabilities. This fact can be used to demonstrate that as certain trust networks grow indefinitely, their trust properties are not certain to be present.

Keywords: Trust, formal logic

1. Introduction

Over the years, trust has proved to be a hard to formally define concept for traditional computing systems and networks as well as the recent grid computing paradigm.

[1]Partially supported by the IST Programme of the European Union under contact number IST-2005-15964 (AEOLUS) and the INTAS Programme under contract with Ref. No 04-77-7173 (Data Flow Systems: Algorithms and Complexity (DFS-AC)).

Given this limited definability, trust has typically be based on establishing mechanisms of authentication, security, and privacy. In addition, trust is also linked to other equally hard to define concepts such as honesty, reputation and reliability. However, trust plays a major role in the viability and usability of a computing system. For instance, in an ad-hoc network, where there are numerous dynamically changing interactions between the participating entities, trust is a fundamental challenge to establish and deploy. Thus, there seems to be a need for a general trust evaluation model that can also reflect the highly dynamic nature of modern computing environments.

Our focus in this paper is on trust models that support unpredictable (i.e. random) interactions between elements of a dynamic distributed computing system such as ad-hoc and wireless network. Our approach can be paralleled to the trust model given in [Mahoney G et Al.(2005)] that attempts to define trust as the result of the interactions between pairs of network nodes, where each interaction is of the form $< l, c >$ with l being the trust level and c the confidence in this level. With regard to other work on trust, there is considerable ongoing research on the development and analysis of new trust management models. Blaze *et al.* in [Blaze M. et Al (1996)] proposed the application of automated trust mechanisms in distributed systems. Josang [A. Josang (1996)] focus on the strong relationship between the notions of trust and security. Moreover a number of schemes for the design of secure information systems have been proposed (see,for example [Eschenauer L. et Al. (2002)] and [Hubaux J. et Al. (2001)]) which are based on automated trust management protocols. The composition and propagation of trust information between elements of information systems are also of pivotal concern and a number of research works are devoted to them (see [Guha R. et Al. (2004)],[Richardson M. et Al. (2003)]). Marsh in [Marsh S. (1994)] makes a first attempt to formalize *Computational Trust* using definitions or rules for representing and evaluating trust-like relationships.

In our work, we rely on formal logic and the theory of threshold phenomena that asymptotically emerge with certainty (under certain conditions) in order to build new trust models and to evaluate the existing one. We try to combine first and second order logic in order to analyze the trust measures of specific network models. Moreover we use formal logic in order to determine whether generic reliability trust models provide a method for deriving trust between peers/entities as the network's components grow.

Moreover we analyze two different graph models, the first one is : *Intersection Random Graph* model, denoted by $G_{k,m,p}$, and the second one is: *Fixed Radius Random Graph*, denoted by $G_{k,R0,2}$. According to the former model, each of the *k* agents selects uniformly at random a subset from a set of m available resources, each of which selected independently of the others with probability *p*. Then two agents are lined via a ‘‘trust’’ edge whenever their selections contain at least one common resource. According to the latter model, *k* agents are placed uniformly at random within a circular area of radius R_0 and two of them are lined via a ``trust" edge if their distance is at most *R₀=2C*. Then using a number of natural, formally definable properties of these models we can define global ‘‘trust’’ system properties that emerge though the local trust interactions (trust edges of the model) under certain conditions.

2. The first and second order languages of graphs

2.1 First order language of graphs

In this subsection we will be focused on graph properties expressible in the *first order language* of graphs. This language can be used to describe some useful (and naturally occurring in applications) properties of random graphs under a certain random graph model using elements of the first order logic.

We will now define the important *extension statement* in natural language, although it clearly can be written using the first order language of graphs (see for the details [Spenser J. (2001)]):

Definition 1 (Extension statement $A_{s,t}$) *The extension statement $A_{s,t}$, for given values of s,t, states that for all distinct $x_1,x_2,\dots,x_s$ and $y_1,y_2,\dots,y_t$ there exists distinct z adjacent to all x_i s but no y_j.*

The importance of the extension statement $A_{r,s}$ lies in the following Theorem.

Theorem 1. *Let G to be a random graph with n nodes and $A_{r,s}$ to be an extension statement, then if $A_{r,s}$ for all r,s $\lim_{n\to\infty} Pr[GhasA_{r,s}]=1$, then for every statement A written in the first order language of graphs either $\lim_{n\to\infty} Pr[GhasA]=0$ or $\lim_{n\to\infty} Pr[GhasA]=1$.*

The connection between threshold properties and first order logic was first noted by Fagin in the seminal paper [Fagin R. (1976)]. In Section 4 we will describe a simple trust model based on the intersection random graph model.

2.2 Second order language of graphs

Although the extension property can be used in order to settle the existence of thresholds for all properties expressible in the first order language of graphs in any random graph model, things change dramatically when properties are considered that are expressed in the *second* order language of graphs.

The second order language of graphs is defined exactly as the first order language (see Section 2.1) except that it allows quantification over subsets of graph vertices (predicates) instead of single vertices. An example of such a property follows (see e.g. [Gupta et Al (1998)]).

Definition 2 (Separator property) *Let $F = \{F_1, F_2, \ldots, F_m\}$ be a family of subsets of some set X . A separator for F is a pair (S,T) of disjoint subsets of X such that each member of F is disjoint from either S or from T . The size of the separator is* $\min(|S|,|T|)$.

In order to cast the separator property into the language of graphs, we set X to be a set of vertices and the subsets F_i to be of cardinality 2 so as to represent graph edges. Then the separator property can be written in the framework of the second order language of graphs as follows:

$$\exists S \exists T \forall x \forall y [\neg(Sx \wedge Tx) \wedge (Axy \to \neg(Sx \wedge Ty \vee Sy \wedge Tx)]. \quad \textbf{(1)}$$

Let us define another property:

Definition 3 (Vertex attractor property) *A graph G has the trusted representatives property if there exists a set of vertices such that any vertex in the graph is an adjacent with at least one of these vertices.*

A formal definition using second order logic is the following:

$$\exists S \forall x \exists y [Axy \wedge Sy]. \quad \textbf{(2)}$$

The extension statement, cannot, unfortunately, be used in order to examine whether (and under which conditions on the random graph model parameters) the separator property or the trusted representatives property is a threshold property since these properties cannot be written in the first order language of graphs. However, there are second order fragments that do not have a threshold behavior while other second order fragments do (see [Kolaitis et Al. (1987)] , [Kolaitis et Al. (2000)]).

Let Σ_1^1 denote the existential second order logic (i.e. formulas contain only existential quantification over second order variables, that is sets). Let FO denote the first order logic formalism and L be any fragment of FO. Then a $\Sigma_1^1(L)$ sentence over a vocabulary R is an expression of the form $\exists S \phi(R,S)$, where S is a set of relation variables and $\phi(R,S)$ is a first order sentence on vocabulary (R,S) (see [Kolaitis et Al. (2000)]).

3. Confidence based trust models and Kernel properties of directed graphs

We can consider a network of trust as a labeled directed graph where the edge labels indicate the trust levels. Let $G = (V(G), E(G))$ to be such a directed graph, where $V(G)$ represents its vertex set and the $E(G)$ the set of arcs. We will use a slightly adapted version of the trust model defined in [Mahoney G. et Al. (2005)] in order to show that some trust definitions lead to trust models that have no asymptotic probabilities for their properties.

Definition 4. *If* $v_1, v_2 \in V(G)$ *and* $(v_1, v_2) \in E(G)$ *then the label* $< l, c >$ *denotes* v_1*'s trust and confidence in* v_2. *Each arc* $(v_1, v_2) \in E(G)$ *has a label of the form* $< l, c >$, *where:*

- $l > 0$ *is the level of trust of* v_1 *in* v_2.
- c *is a confidence value in* $[0,1]$.

The *Kernel* property, which we believe can be the prototype for discovering other non-threshold properties, is defined in the context of directed graphs. The language of directed graphs is the same as the language of undirected graphs with only difference that the predicate $A_{x,y}$ that signifies adjacency between x and y is not symmetric. A random digraph, according to model $G_{n,p}$ is constructed by having each of the possible, directed edges being chosen for inclusion independently of each other, with constant probability p. Then a kernel in the produced directed graph is a subset U of the set of vertices such that no edge exists between vertices within U while for each vertex outside U there exists an edge from this vertex to some vertex within U. This property is given below, written in the second order language of graphs (see [Mahoney G. et Al. (2005)]):

$$\exists U[(\forall x \forall y((Ux \wedge Uy) \to \neg A_{x,y})) \wedge (\forall x \exists y(\neg Ux \to (Uy \wedge A_{x,y})))]. \qquad \textbf{(3)}$$

The property in (3) is written in $\Sigma_1^1(FO^2)$, with FO^2 being the fragment of first order logic allowing propositions containing at most 2 variables. This property has asymptotic probability 1. However, in [Le Bars J.-M et Al (1998)] (see, also, [Le Bars J.-M et Al (2000)]) two variants of the Kernel property were proposed that have *no* asymptotic probability and which are directed related to trust within the context of the model described in Section 4. We will concentrate below in the first variant, K_1.

Let $R = \{R_1, \ldots, R_{16}, S_1^1, \ldots, S_{16}^1, \ldots, S_1^{2^{15}}, \ldots, S_{16}^{2^{15}}\}$ be a set of vocabulary symbols.

We define K_1 on finite structures over the vocabulary R. An R-structure M_n on domain n satisfies K_1 if it has at least one kernel U, i.e. a subset of the n parts of the structure that satisfies the following *INSIDE* and *OUTSIDE* properties:

- INSIDE: No pair of distinct elements (a,b) of $U \times U$ belongs to $\bigcup_{i\in\{1,2,\ldots,16\}} R_i$.

- OUTSIDE: For any $j \in \{1,\ldots,2^{15}\}$ and any vertex c of $n \setminus U$, there is a vertex $d_j \in U$ such that (c,d_j) belongs to $\bigcup_{i\in\{1,2,\ldots,16\}} S_i^j$.

The property K_1 is, now, expressible by the following $\sum_1^1(FO^2)$ R-sentence

$$\exists U(\left(\forall x \forall y \left(Ux \wedge Uy \wedge x \neq y\right) \rightarrow \neg\left(\vee_{i\in\{1,\ldots,16\}} R_i xy\right)\right)$$
$$\wedge\left(\wedge_{j\in\{1,\ldots,2^{15}\}} \forall x \exists y \left(\neg Ux \rightarrow \left(Uy \wedge \vee_{i\in\{1,\ldots,16\}} S_i^j xy\right)\right)\right)). \quad \textbf{(4)}$$

In the context of the trust model given in Definition 4, we can think as follows. For the labels $< l, c >$, we let l take values on the discrete value set $\{1,2,\ldots,16\}$ while the confidence value c is suitably discretized within the range $[0,1]$, so as to take values on the discrete value set $\{1,2,\ldots,2^{15}\}$.

The vocabulary $R = \{R_1,\ldots,R_{16}, S_1^1,\ldots,S_{16}^1,\ldots,S_1^{2^{15}},\ldots,S_{16}^{2^{15}}\}$ can be partitioned into the following 17 sets:

$$R_1 = \{R_1,\ldots,R_{16}\}, S_1 = \{S_1^1,\ldots,S_1^{2^{15}}\}, S_2 = \{S_2^1,\ldots,S_2^{2^{15}}\},\ldots, S_{16} = \{S_{16}^1,\ldots,S_{16}^{2^{15}}\}.$$

The R set represents the 16 levels of trust with 0 confidence level. The 16 S sets represent the 16 possible levels of trust and their members correspond to the 2^{15} possible non-zero confidence values.According to the above formulation, the property K_1 says that there is a subset U of the n parts of the structure that are not pairwise connected with trust labels from the class $\bigcup_{i\in\{1,2,\ldots,16\}} R_i$, i.e. the confidence value of their pairwise trust levels is non-zero, while every possible non-zero confidence level, from 1 to 2^{15}, is present in at least one trust connection from a non-member of U to a member of U. Using the main result of [Le Bars J.-M et Al (1998)] that the property K_1 does not have a limiting probability and, thus, in particular cannot hold with probability 1, we deduce that the the analogous trust property we described within the K_1 context also does not hold with probability tending to 1 as the system's size n increases.

Although this connection of the trust model in Definition 4 with the property K_1 is not very natural it, nevertheless, shows that one can describe trust relations that do not have a limiting probability as the trust structure grows and the interactions vary in an unpredictable (i.e. random) fashion. We believe that one can use this connection, however, in order to establish other more natural properties that, also, do not possess a limiting probability and, thus, are not guaranteed to hold with certainty in the limit.

4. A generic trust model based on threshold laws for mathematical logic

As we mentioned earlier in this paper, trust is a difficult concept to formalize and handle. What is more, our target framework of global/dynamic computation clusters does not seem to allow a static view of the trust concept, regardless of the way in which this concept is formalized. Our viewpoint is that trust should be a statistical, asymptotic concept to be studied in the limit, as the system's components grow according to some growth rate. Our practical viewpoint of trust in a dynamic, global computing system is the following :

i)First one adopts a suitable random graph model that best suits the target dynamic system (network).
ii) Secondly, one is focused on defining a number of properties that model facets of trust using first order logic or some second order logic fragment. Examples of such properties is the triangle property given in Section 2.1 and the separator and trusted representatives properties defined in (1) and (2) in Section 2.2 . If the property can be cast into the first order language of graphs, then one is certain that this is a certain property that either is possessed almost certainly by the growing system or it is not possessed almost certainly, depending on its monotonicity.
iii)Following the second step, if the property under consideration can only be written using second order logic, then one examines whether the property can be cast into the language of a fragment of the second order logic that has a threshold behavior. Then one is certain that as the system grows the property holds asymptotically almost certainly or almost never (again depending on its monotonocity).
However, if the property seems to be describable only in a second order logic fragment that, in general, does not have a threshold behavior) then this property should be further examined as to whether it is a threshold property or not. Such a property, called *Kernel* (see below for a definition) is given in [Le Bars J.-M et Al (1998)] for the $G_{n,p}$ model with fixed p. It is interesting to define second order properties related to trust for a random graph model that have no threshold behavior since they are guaranteed to hold for a positive fraction of the random structures allowed by a random graph model.

5. Trust in Graph Models

Based on the results presented in [Liagkou V. et Al.(2006)]), we will propose below a number of trust-related properties that can be studied in the context of the random intersection graph model and the fixed radius random graph model.

5.1 Trust Properties of Intersection graph model

Let us assume that we have a $G_{k,m,p}$ random graph, interpreting its parameters in the following way. We have k available computing agents and m resources (e.g. trusted service access points or computer ports, located in some server). According to the model, each of the k agents selects uniformly at random from within the set of the m resources, each of which selected independently of the others with probability p. Then two agents are connected with a ‘‘trust’’ edge whenever their selections contain at least one shared service. From this point, we can proceed along two directions using the ideas proposed in the previous sections.

The first direction consists in discovering a number of global system properties related to trust, that emerge through the local trust interactions (trust edges of the model), and define ranges of the model parameters that lead to the almost certain asymptotic validity or non validity of the global property of interest.
For concreteness, let us define the following first order property:

$$\forall x \exists y [A_{x,y}] \qquad \textbf{(4)}$$

which states that for each node x there exists at least one other node such that the two nodes trust each other. Since this property is monotone increasing, if the model parameters k, m, p obey the conditions then as the node population increases, the property stated above holds with probability tending to 1.

Another property that can be defined is the following:

$$\forall x \forall y \forall z [A_{x,y} \wedge A_{y,z} \rightarrow Axz] \qquad \textbf{(5)}$$

which states that the trust relationship is transitive. Again, if the conditions on the random intersection graph model parameters hold, then in the limit the trust relationship is transitive with probability tending to 1. Similarly, the trusted representatives property holds for the random intersection graph model (see discussion in Section 2.2).

5.2 Trust Properties of Fixed radius random graph model

Suppose that we have n agents randomly distributed within a circle of radius R_0 . We first define a circle of radius *C* cantered at each agent. Our fixed radius random graph with *n* agents is formed so as to include ‘‘trust’’ edges between agents only if their distance is at most *2C*. Thus two agents establish a trusted connection if their cycles (of radius C) are intersected. Let us now define some first order properties related to trust using the threshold properties of the fixed radius graph model. In this context, $R_0=2C$, that is two agents that trust each other if their ranges intersect, which occurs if their distance is at most *2C*. Let us consider the following property: *every two vertices have a common trust agent*. If this property holds, then for *each* pair of agents that establish a trust connection there exists another trusted identity. This may cause problems since it increases the number of trusted parties without reason. As they both trust a third agent it is better one of them an indirectly trust connection with the third one. Setting $\frac{C(n)}{R(n)} = O(\frac{1}{\sqrt{n}})$, this property is monotone increasing and it holds with probability tending to 0 (see [Liagkou V. et Al.(2006)]). Thus its complementary property, which is a trust' property, holds with probability 1.

The second direction along which one can proceed is, in some sense, the opposite of the direction outlined above. The goal is not to establish conditions for ensuring almost certain validity or non-validity of some first order property related to trust but, on the contrary, to state higher order properties in the second order language of graphs (like the separator or vertex attractor property given in Section 2.2) and show that the properties have no limiting probability, i.e. they cannot be threshold properties. Such a property, being not a threshold property, leads a complex system to some kind of equilibrium, as the system grows. In both directions given above, the central idea is that trust is global property characterized by local interaction between system entities.

6. Conclusions and directions for further research

In this paper we have attempted to provide a practical and viable definition of trust for dynamically changing computing environments that can be described within the global computing paradigm. Our view is that trust can be reduced to a number of properties that appear as a limiting behavior in systems under certain conditions. These systems are modeled within the formalism of a random graph model according to the context of the target system. Then the properties can be written formally using the first and second order language of graphs. If the properties can be written in the first order language of graphs then one can use the extension statements in order to establish the conditions under which the model displays threshold behavior and, thus, all the properties hold asymptotically with either probability 0 or 1.

We hope that our paper will be a first step towards defining a methodology for studying a variety of properties (not only related to trust) using suitable random graph models and then look at the produced (by the model) systems not individually (which is impossible in a rapidly changing environment) but collectively in the limit.

References

Blaze M., Feigenbaum J., and Lacy J. (1996), *Decentralized trust management*, in IEEE Symposium on Security and Privacy, Oakland (CA, USA), pp. 164--173.Bolloba′s B. (2001), *Random Graphs*, Second Edition, Cambridge University Press.

Fagin R. (1976), *Probabilities on Finite Models*, J. Symbolic Logic 41, pp. 50--58.

Gupta P. and Kumar P.R., ``Critical power for asymptotic connectivity," in *Proc. of Conf. on Decision and Control, Tampa, USA*, 1998.

Kolaitis P.G. and Vardi M.Y. (1987), *The Decision Problem for the Probabilities of Higher-Order Properties*, in Proc. 19th ACM Symp. on Theory of Computing, New York, pp. 425--435.

Kolaitis P.G. and Vardi M.Y. (2000), *0-1 Laws for Fragments of Existential Second-order Logic: A Survey*, in Proc. MFCS 2000, Springer-Verlag, pp. 84--98.

Le Bars J.-M. (1998), *Fragments of Existential Second-Order Logic without 0-1 Laws*, in Proc. 13th IEEE Symp. on Logic in Computer Science, pp. 525--536.

Le Bars J.-M. (2000), *Counterexamples of the 0-1 Law for Fragments of Existential Second-Order Logic: an Overview*, Bulletin of Symbolic Logic 6, pp. 67--82.

Eschenauer L., Gligor V. D., and Baras J. S. (2002), *On trust establishment in mobile ad-hoc networks*, in Proc. Security Protocols Workshop, Cambridge (UK), pp. 47--66.

Guha R.,Kumar R., Raghavan P., and Tomkins A. (2004), *Propagation of trust and distrust*, in Proc. International Conference on World Wide Web, pp. 403--412.

Hubaux J.-P., Buttyan L., and Capkun S. (2001), *The quest for security in mobile ad hoc networks*, in Proc. ACM International Symposium on Mobile ad-hoc networking and computing, pp. 146--155.

Josang A. (1996), *The right type of trust for distributed systems*, in Proc. New Security Paradigms Workshop, pp. 119--131.S. D. Kamvar, M. T. Schlosser, and

Liagkou V., Makri E., Spirakis P., and Stamatiou Y.C. (2006), *The threshold behavior of the fixed radius random graph model and applications to the key management problem of sensor networks*, ALGOSENSORS, pp. 130--139.

Mahoney G., Myrvold W., and Shoja G.C. (2005), *Generic Reliability Trust Model*, In A. Ghorbani and S. Marsh, editors, Proceedings of the 3rd Annual Conference on Privacy, Security and Trust, Canada.

Marsh S. (1994), *Formalising trust as a computational concept*, Ph.D. dissertation, University of Stirling, Department of Computing Science and Mathematics,pp.214.