

Modelling Interactions in Ubiquitous Environments

M. O. Ahmed and S. M. V. Hailes

Department of Computer Science, University College London London WC1E 6BT, UK

{M.Ahmed, S.Hailes}@cs.ucl.ac.uk

I. INTRODUCTION

In all computer systems, interactions between parties require the establishment of a level of trust that is determined to be sufficient to permit the requested action to take place. Traditionally, such trust has been policed centrally by having authorities that determine whether or not an individual is trustworthy (cf Equifax etc.). To make this work, several premises must hold: (1) there is widespread trust in such authorities (2) the penalties that the central authorities can impose by withdrawing their sanction are sufficiently severe as to discourage bad behaviour (3) it is not possible for individuals to easily change their identity to avoid such penalties. It is questionable whether these premises are met in existing networks; however, in ubiquitous computing environments, they are highly unreasonable as general assumptions (which is not the same thing as saying that such central authorities can never exist or be useful). Thus, in order to build truly ubiquitous systems, it is necessary to develop decentralised security mechanisms that give useful information about trustworthiness in the absence of a central point of reference or control.

Ensuring cooperation by evaluating likely trustworthiness locally has formed the basis of a number of studies [2], [5], [10], [11]. A large body of research has also focused on creating algorithms that evaluate trust incrementally based on induction based over a history of direct observations and the testimonies of witnesses [1], [2], [9], [12], [13], amongst others. These studies, however, ignore two important factors: firstly the effect of the physical, behavioural and organisational constraints of components in creating sustainable decentralised trust-based mechanisms, and, secondly, the influence of the embedded social networks from which witnesses are derived in facilitating cooperation and gathering information about prospective trustees.

Cooperating through trusting intentions carries greater perceived risk than centrally managed trust, because policies are local, policy violation is local, and consequently enforcement is local. This is in part due to our self-imposed constraint that insists that we do not rely on centralised trusted bodies. However, in game theoretic terms, this leads to the problem that opportunism becomes the dominant strategy, especially when interactions are unpredictable or infrequent [4] in view of the fact that memory constraints may limit the length of history that principals can hold. This, combined with the discounting of the payoffs for interaction in the far future makes reciprocity alone an unrealistic strategy for facilitating cooperation.

The difficulty here is that the perception of risk is actually wrong; the attempt to assure certainty in trust through centralisation is only superficially equivalent to the control of risk. In reality, risk is multi-dimensional (it applies differentially in different contexts of application) and inherently local (not all trusting decisions can be delegated). Ignoring these factors does not actually make the control of risk any simpler, though it gives the appearance of having done so; it just results in the use of an inappropriate oversimplification. As Braynov et al. state:

“... In risky environments, trust enables cooperation and permits voluntary participation in mutually beneficial transactions which are otherwise costly to enforce or cannot be enforced by third parties.” [3]

Thus trust/reputation management mechanisms are inherently concerned with addressing the problem of risk reduction in interaction. However, as a number of highly cited theoretical examinations of trust show [6], [7], [8] (amongst others), to make this work it is essential to consider:

- 1) The need for a credible threat of punishment to facilitate cooperation by making compliance with the terms of a transaction an incentive for gaining access to further transactions
- 2) The high value of the embedded social network of principals as a source of high quality information.

The former point is no different to the premise on which the centralised trust approach is based. It is frequently argued that the lack of assurance of identity or the lack of an incentive to maintain a consistent pseudonym is a problem for this environment since it allows individuals to avoid punishment. However, this misses the point somewhat. There is no *requirement* on principals to accept a weaker form of assurance about identity than in any centralised system; however, if they *choose* to do so, then it is desirable to ensure that there are still consequences to cheating resulting from collective approbation of, of exclusion from, a community that has value to its members. Since these sanctions can, at best, be applied to a pseudonym, their true cost to the attacker lies in the cost of re-establishing the same degree of trust that was abused. Thus, *caveat venditor*.

II. SOCIAL NETWORKS

Social network theories such as *cohesive groups* suggest that trust and its global incarnation (reputation) are in part group-based (embedded in the social network from which information is gathered) and that these groups can offer dense information channels that keep members up to date while creating an inherent control mechanism in the form of gossip and collective reward or punishment i.e. increased or reduced levels of cooperation. However these theories do not offer any concrete methods for

creating such mechanisms, but are the result of observation-based analysis. So, questions such as: what environmental constraints affect the formation of persistent trust based mechanisms; what is the nature of trust/reputation in such groups or how can this information be integrated into evaluating trust and reputation (if at all) are open to discussion.

The intuition behind this work is that mechanisms such as cohesive groups which, essentially act as incentives to cooperate in the environment are the products of emergent behaviours. They are realised through understanding the effects of the constraints in the environment and the topology of interactions. We therefore present a model of trust management that translates the consequences of interactions between participants from private to public. To facilitate this, we divide the interaction process into three stages: (1) the interaction between a principal and a trustee, which is treated as a signalling game in which the trustee tries to maximise the chances of its request being granted and the principal tries to minimise the threat posed by the actions granted; (2) the interaction between a principal and a witness, which can be treated as cheap-talk game; (3) the process of self organisation in which principals proactively select the participants from whom they obtain testimonies and reputation. These latter processes are outside the scope of this short paper; however, the formulation below presents the first interaction model, were, the timing of the game follows the traditional signalling game procedure. Given:

- A security categorisation, sec , is a tuple consisting of the objective and an impact level for each objective:

$$\begin{aligned} \text{Objective } OBJ: & \quad OBJ = \{confidentiality, integrity, availability\} \\ \text{Impact } IMP: & \quad IMP = \{high, moderate, low, null\} \\ \text{A categorisation } (sec): & \quad sec_{act_i} = \{OBJ, IMP\} \end{aligned}$$

- An action is an atomic element representing a manipulation of a resource. Each action (act_i) has associated with it a pre and post-condition and a security categorisation representing the maximum threat it poses to the resource.

$$\begin{aligned} \text{A procedure } (proc): & \quad \forall act_i \exists proc_i & \text{A post-condition } (post): & \quad \forall act_i \exists post_i \\ \text{A pre-condition } (pre): & \quad \forall act_i \exists prec_i & \text{A security categorisation } (sec): & \quad \forall act_i \exists sec_{act_i} \end{aligned}$$

The interaction between a principal (a_p) and a trustee (a_x) is determined by:

$$\begin{aligned} \text{Types of agents:} & \quad T = \{malicious, good\} & \text{Identity of trustee:} & \quad a_x \\ \text{Set of principals' actions:} & \quad AC = \{believe, disbelieve\} & \text{Request for an action:} & \quad req(a_x, act_i, \gamma_i) \\ \text{Set of resources:} & \quad \Gamma_p = \{\gamma_1, \gamma_2 \dots \gamma_n\} & \text{Trust in trustee:} & \quad tr\{a_p, a_x, \gamma_i\} \\ \text{Utility of trustee:} & \quad U_x(t_x, req_x, act_i) & \text{Utility of principal:} & \quad U_p(t_x, req_x, act_i) = \min_{act_i \in AC} \{sec_{act_i}\} \end{aligned}$$

$$\begin{aligned} \text{Principal's belief in type of } a_x: & \quad \mu_{t_x \in T}(t_x | req_x) \propto tr\{a_p, a_x, \gamma_i\} \\ \text{Principal's utility maximisation function:} & \quad a^*(req_x) = \max_{act_i \in AC} \{g(\mu_{t_x \in T}(t_x | req_x), U_p(t_x, req_x, act_i))\} \\ \text{Trustee's utility function:} & \quad \max_{\forall req} \{U_x(t_x, req_x, a^*(req_x))\} \end{aligned}$$

III. CONCLUSION

In this short paper, we motivated the need for distributed trust management in ubiquitous computing environments and identified the central role to be played by social networks in this. In support of this, we introduced a game-theoretic formulation of the interaction between principals and trustees.

REFERENCES

- [1] A. Abdul-Rahman and S. Hailes. Supporting trust in virtual communities. In *The 33rd Hawaii International Conference on System Sciences*, Maui, Hawaii, January 2000.
- [2] M. Blaze, J. Feigenbaum, and M. Strauss. Compliance-checking in the policymaker trust-management system. In *2nd Conference on Financial Cryptography*, 1998.
- [3] S. Brainov and T. Sandholm. Contracting with uncertain level of trust. In *The first ACM conference on Electronic commerce*, DenverUSA, November 1999.
- [4] R. Burt. Private games are too dangerous. *Computational and Mathematical Organization Theory*, 1999.
- [5] Y. Chu. Referee: Trust management for the world wide web. Master's thesis, MIT, June 1997.
- [6] J. Coleman. Social capital in the creation of human capital. *American Journal of Sociology*, 94, 1988.
- [7] P. Dasgupta. Trust as a commodity. In D. Gambetta, editor, *Trust: Making and Breaking Cooperative Relations, electronic edition*, chapter 4, pages 49–72. Department of Sociology, University of Oxford, <http://www.sociology.ox.ac.uk/papers/dasgupta49-72.pdf>, 1988/2000.
- [8] M. Granovetter. Economic action and social structure: The problem of embeddedness, 1985.
- [9] A. Josang and R. Ismail. The beta reputation system. In *15th Bled Conference on Electronic Commerce*, Bled, Slovenia, June 2002.
- [10] L. Kagal, T. Finin, and A. Joshi. Moving from security to distributed trust in ubiquitous computing environments. *IEEE Computer*, December 2001.
- [11] S. P. Marsh. *Formalising Trust as a Computational Concept, in Computing Science and Mathematics*. PhD thesis, University of Stirling: Stirling, Scotland, 1994.
- [12] B. Shand, N. Dimmock, and J. Bacon. Trust for transparent, ubiquitous collaboration. In *First IEEE Annual Conference on Pervasive Computing and Communications (PerCom 2003)*, pages 153–160, Dallas-Ft. Worth, TX, USA, March 2003.
- [13] B. Yu and M. P. Singh. A social mechanism of reputation management in electronic communities. In *Fourth International Workshop on Cooperative Information Agents*, pages 154–165, 2000.