

## Trust-Based Admission Control in Collaborative Ad Hoc Applications

Elizabeth Gray<sup>1</sup>, Paul O'Connell, Christian Jensen<sup>2</sup>, Stefan Weber, Jean-Marc Seigneur, Yong Chen

<sup>1</sup>Distributed Systems Group, Department of Computer Science,

Trinity College Dublin, Ireland. Email: [grayl@tcd.ie](mailto:grayl@tcd.ie)

<sup>2</sup>Informatics and Mathematical Modelling, Technical University of Denmark. Email: [cdj@imm.dtu.dk](mailto:cdj@imm.dtu.dk)

The proliferation of mobile devices and the development of networking technologies has introduced the possibility of a vast, networked infrastructure of diverse entities partaking in collaborative applications with each other. However, this may require interaction between users who may be marginally or completely unknown to each other, or interaction in situations where complete information is unavailable. A mobile ad hoc network is an autonomous system of mobile entities connected by wireless links. The entities are free to move randomly and are self-organising, so the network is highly dynamic and subject to rapid and unpredictable changes. As in traditional networks, access to collaborative resources in mobile ad hoc networks requires varying levels of control. Difficulties arise, however, when traditional access control methods are applied in a decentralised collaborative ad hoc environment. For example, in traditional groupware applications, access to a group is controlled by an administrator with a predefined list of possible group members. The administrator grants access rights based on whether the requesting entity is identified as meeting the appropriate criteria. Access control based on the centralised administrator model becomes ineffective, however, in a vast networked infrastructure of diverse entities partaking in collaborative applications with one another on an ad hoc basis.

For example, suppose Alice takes the 8am commuter train into the city to work every weekday morning. To pass the time, she wishes to play an interactive game with other train passengers. She joins an ad hoc wireless network to see what collaborative gaming applications are available. She discovers an ongoing blackjack session in which Bob is the dealer, and she requests admission to the game. To Bob, Alice is an unknown entity, who may or may not be trusted to behave correctly, i.e. pay her debts, if given access to his game. In the traditional model, Bob would be able to contact a centralised administrator to determine if Alice should have access rights to participate in the blackjack game. Ultimately, making the traditional model work in this scenario would require a global authorisation structure, since Alice and Bob may live in different countries and only be meeting by chance. This approach does not scale to the large, dynamic, decentralised ad hoc networks envisioned.

Trust has been well-researched in another kind of massive ad hoc collaborative network infrastructure. Humans must regularly determine with no assistance from a trusted third party, how to interact with known and unknown people. Trust provides a mechanism for lowering access barriers and enables complex transactions between groups. Humans use the concept of trust to help decide the extent to which they cooperate with others in these types of situations, where complete information is not available. It provides a mechanism for lowering access barriers and enables complex transactions between groups. Human trust, however, takes many different forms and is difficult to stringently define or understand.

We are currently developing a system that enables access control based on the human notion of trust through admission policies that define the trust relationship between entities in collaborative ad hoc applications. We do this by integrating a trust-formation element into an admission control mechanism to manage interaction between known and previously-unknown users. Initial evaluation of this system is based on a simple distributed blackjack card game application, which implements the trust-based admission control system to assign roles to users according to their trust-based admission rights. Results of the evaluation show that our prototype reacts correctly to user behaviour, i.e. the system adjusts trust values and implements admission policies similar to human trust assessment.