A Framework for the Decentralisation and Management of Collaborative Applications in Ubiquitous Computing Environments

Karl Quinn, Austin Kenny, Kevin Feeney, David Lewis, Declan O'Sullivan, Vincent P. Wade
Knowledge & Data Engineering Group,
Department of Computer Science,
Trinity College Dublin,
Dublin, Ireland.
{Karl.Quinn | kennyau | Kevin.Feeney | Dave.Lewis | Declan.OSullivan | Vincent.Wade}@cs.tcd.ie

Abstract—**When deploying collaborative applications such as Instant Messaging in ubiquitous computing environments significant enhancements can be afforded by offering additional context information, such as location information. However, such environments exert key challenges such as increased diversity of ownership and ad hoc, intermittent network connectivity that suits more decentralized computing architectures. This paper examines how a migration to a more decentralized collaborative architecture can be achieved together with a decentralization of the management of collaborative activities.**

Keywords; Collaborative Application, Trust, Community-based Management, Content-Based Networking, Instant Messaging.

I. Introduction

File sharing and file distribution has been decentralised through the user of a peer-to-peer communications architecture. Currently, Instant Messaging (IM) applications use centralized architectures. We provide a framework for decentralizing IM applications in terms of its message routing and management. However, this IM application is only one instance of many application areas that can take advantage of this framework. For instance, we could also decentralize and manage Voice over Internet Protocol (VoIP), email, RSS feeds, etc, which all operate over centralized, client-server, architectures, similar to IM. A Content Based Network (CBN) [1] provides a flexible mechanism for dynamically configuring need patterns of communication between groups of users.

Access control in systems such as IM or VoIP is centralized. This framework enables access control to be decentralized, which places it into the hands of the user. Furthermore, the administration or management of access control policies is also decentralized. Policy based management has the potential to enable communities and individuals to exercise a high level of control over managed information resources. However, this potential will only be realized in collaborative applications if the management systems are properly integrated with the human communities within which they are deployed. In particular, the management of collaborative applications should focus on the human relationship that the system supports rather than being presented in terms of the underlying computing resources that mediate the collaboration. This allows management policies to be stated in terms that are directly meaningful to the collaborating user. However this requires that the policy-based management system used is flexible enough to accommodate the myriad of ways in which humans naturally communicate.

We focus on managing collaborative applications, such as IM, in a ubiquitous computing setting where mobile users and equipment can further enrich the modes of collaboration available to the user. This paper presents a framework that allows centralized collaborative applications to be migrated to a decentralized, ubiquitous computing, architectures. The framework also provides a mechanism that empowers community members to model their community hierarchy, which reflects the natural community structure. Interactions between collaborative applications are managed by enabling the community to regulate access control. Access control is based on a trust model that is personalized on a per user basis.

Section II examines the CBN research. Sections III and IV examines Community Based Policy Management (CBPM) and Trust Based Access Control (TBAC), respectively. Section V presents the integrated system in operation and VI concludes.

II. Decentralizing the Collaborative Medium

Instant Messaging (IM) has become an influential part of both consumer and commercial collaborative activities. Similar to email it provides a powerful desktop communication service. In our research we have adopted the XML based JABBER IM which uses the Extensible Messaging and Presence Protocol (XMPP) [2] for streaming XML elements. XMPP establishes a universal messaging address which supports the concept of presence [2]. Presence allows JABBER clients to ascertain what client applications are online and their status. An IM client has a roster of buddies, which are grouped in lists e.g. friends, work colleagues and family.

This research has combined the IM platform JABBER with a CBN infrastructure. This allows the routing of certain messages between collaborating users to be undertaken by a decentralized network of content-based routers rather than relying on a single IM server. CBNs provide content-delivery

1-4244-0143-7/06/$20.00 ©2006 IEEE

via a publisher/subscriber model [1]. Whereas OASIS [3] utilizes CBN technology with access control preformed on the CBN broker side. Routing decisions in a CBN our made based on content rather than traditional physical address based routing. Subscribers are allowed to express their interest in event content. This provides a much higher degree of robustness to failure and reduction of performance bottlenecks.

In the context of the IM application the CBN provides access to decentralized trust and policy information. By decentralizing the collaborative management functions of the IM server we aim to establish a flexible migration path to a more resilient and efficient collaborative infrastructure.

III. Community Based Policy Management

In [4] a community-based model for the management of policies in organizations with a decentralized and evolving structure is presented. From this model a framework has been implemented to help policy-driven self-managed systems mediate with organizations in defining management policies in the context of continual organizational change. In addition the framework assists in the resolution of organizational conflicts in the management of resources that arise as a result of the continual change. The community-based abstraction is used to overcome the difficulties in regards a rigidity to change that role based policy systems exhibit. The community-based framework reflects the way humans have traditionally interacted with organizational policy as described by Djiker and Barrett [5]. In the community abstraction all the stakeholders are grouped together in all of the policy decisions. Policies applied at general levels of the organization allow the behaviour of more specific groups to be bounded by general rules. The fluid evolutionary approach to building organizational structure reflects a progressive grounding approach, where policy sets develop over time. This community abstraction was initially developed through observation of the operations of loose Internet based communities [4]. This type of organization represents an extreme in terms of its organizational form in conventional terms; however the flexibility, dynamism and complex distribution of authority of these communities are increasingly represented in traditional forms of organization and will. We believe that this will become the norm in ubiquitous computing operations as collaborations are increasingly formed in an increasingly ad hoc fashion, outside of the scope of a single organization and its collaborative and management infrastructure.

In the context of the IM application the communities form the basis for roster management, thus ensuring consistent view of collaborative grouping across users. Thus roster management reflects the multi-way relationships characteristic of collaboration, rather than the subjective grouping approach found in individual's roster group structures.

IV. Trust Based Access Control

For the IM application we will utilize a dynamic, flexible, personalized, human-centric, model of trust to empower access control decisions across communities, guided by individual and community policies. Our approach to modelling trust attempts to mirror the human model in definition, representation, calculation, and outcome. In [6], [7], and [8] we describe a trust management application that provides a trust based selection process that can assess a range of similar resources and select the appropriate resource specific to the user's trust requirements. We have designed, developed, implemented, and analysed an experiment that validates this approach to modeling trust. Our current and future research work will enable users to create their model of trust, which can be altered over time as the user sees fit. The benefit of using policies to underpin the implementation of the model of trust is that the adaptive nature of these models can be accurately reflected. As the individuals' idea of trust changes, via context or human nature changes, the policies can be easily altered.

In the context of the IM application, trust based access control gives the potential for more fine-grained, but intuitively governed management of rosters. In particular it goes beyond the binary categorization of potential collaborators but inclusion, or not, in a roster. By using individual or community policies to make decision about the visibility given to other who may not be well known, the dynamic development of relationships between collaborators may be accurate reflected. The trust values generated allow individuals and communities to define policies governing the level of access to presence and location information as well as roster membership to users in the same communities or in other communities, including the global community of potential collaborators of which anyone may be a member.

V. Integrated System Operation

We are exploiting the flexibility of our IM Trust based access control and community managed system via a content based network. We in turn promote the migration of current client-server architecture of IM to a platform which is decentralized and more compatible with ubiquitous architectures. Decentralizing architectures brings content closer to the user, increasing the accessibility of the content by any device or network. As well as a real world IM test bed, the access node and CBN uses a virtual test bed. The implementation of a virtual test bed is used for evaluating human interaction with ubiquitous computing environments. This evaluation takes place in a virtual simulator [9]. In this case the simulator provides a means of collecting rich location and personal information in a controlled environment before deploying to a live site. As well as providing live deployment testing it also has the capability of devising a multitude of different scenarios. The CBN we have used in this system is Elvin [1]. Elvin is a client-server system, and thus relatively centralized, albeit with federation possible between servers. Though this makes for similar architecturally to the current client-server architecture defined for XMPP, it provides us with a stable research platform before progressing to more decentralized and ad-hoc CBN architectures, for example Sienna [10], Gryphon [11] and XNET [12].

The access node infrastructure acts as a JABBER proxy for IM applications which allows collaborative application messages to be routed either via JABBER or the CBN. The access node also provides the point of coordination between

1-4244-0143-7/06/$20.00 ©2006 IEEE

the collaborative infrastructure consisting of IM, the CBN, and the management infrastructure. The Communication architecture from client to access node is utilizing the Enterprise Java Bean architecture (EJB) message-driven beans. This provides architecture for investigating the co–existence of CBN and JABBER, with the CBN the JABBER functionality is migrated to a more ad-hoc, decentralized implementation. For simplicity figure one only shows single instances of servers, services, nodes, CBN's, etc.

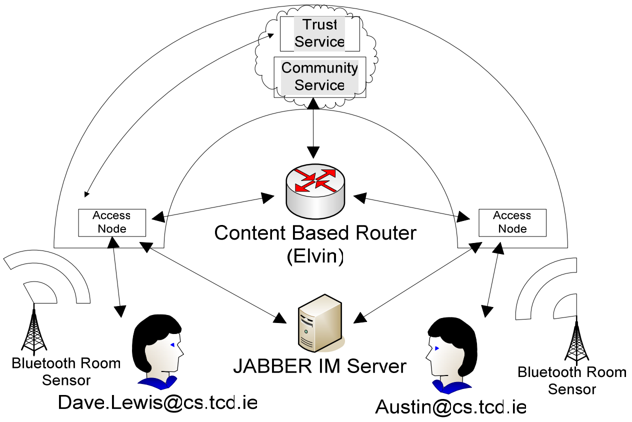

Figure 1. Overall Architecture

As a scenario consider attending a conference where members are obliged to complete a registration procedure. Contained in the registration process members use the community service indicating the communities they are associated with i.e. Programme Committee, IEEE Group, Chair Person or Presenter. Members are outsourced to the community service and formulated into their respective conference communities (see figure 2). At this point members can vote and associate interpretable policy rules to their personal information i.e. *dave.lewis@cs.tcd.ie* during the conference only allows members of the KDEG community to be informed of his location. This generates the opportunity to produce a dynamic roster list adding further functionality to the XMPP roster management, such that *dave.lewis@cs.tcd.ie* has *karl.quinn@cs.tcd.ie* as a member of his KDEG roster community. The community service propagates individuals dynamic roster group to the access node where the roster group is forwarded on behalf of the client to the JABBER server. Such roster changes will not interfere with the user's personal roster groups i.e. friends and family. When the conference is finished the dynamic roster group will be removed from the member's roster list.

In figure 2 Dave (*dave.lewis@cs.tcd.ie*) is a member of both the KDEG and the conference community. KDEG members, including Karl (*karl.quinn@cs.tcd.ie*), can access Dave's location aware information. By default all members of the conference community can send an Instant Message to Dave. However, Dave has explicitly created a rule so that the conference members can not gain access to his location information. The Chair (*chair.person@noms2006.org*) wishes to attain such location information for Dave but they do not know each other directly. Karl knows and has a high trusts regard for the Chair and in turn Dave knows and has a very high trust regard for Karl. It is therefore possible for Dave to calculate a trust value for the Chair via the trust Dave holds in Karl and the trust Karl holds in the Chair. If this calculated trust value meets Dave's minimum requirements for accessing his location information then the Chair can receive Dave's location information.

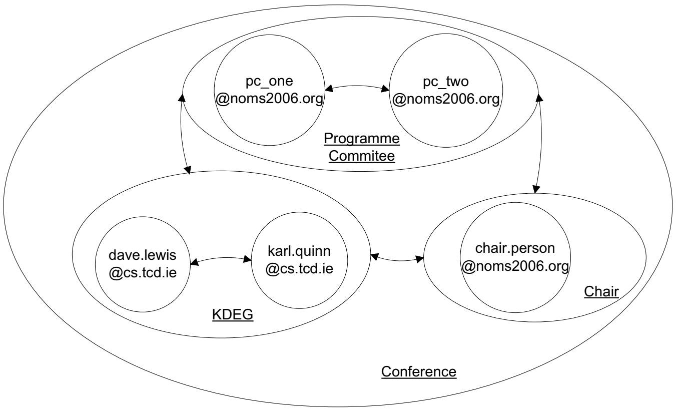

Figure 2. Conference Scenario

The trust management system enables us to ask who knows *dave.lewis@cs.tcd.ie* and get a set of users that may choose to collaborate and answer the query to provide trust data for *dave.lewis@cs.tcd.ie*. The trust management system's search service is based on the collaborative efforts of the community and users can opt out if desired, therefore respecting a users privacy. When searching in a Friend-Of-A-Friend fashion, the search method asks who is a buddy of 'A' and who is a buddy of 'C' and the intersection of these lists becomes user(s) 'B'.

The trust management system provides the ability to calculate a trust value between two users. Once the search has returned a list of buddies that know 'A' we can calculate each buddies trust value for 'A', assuming that they collaborate and provide trust information. In this way we build up a set of trust values that user have in 'A', which we can then present as a final trust value to the user. The trust calculation is based on the personalized model of trust that the user who asked the original query holds.

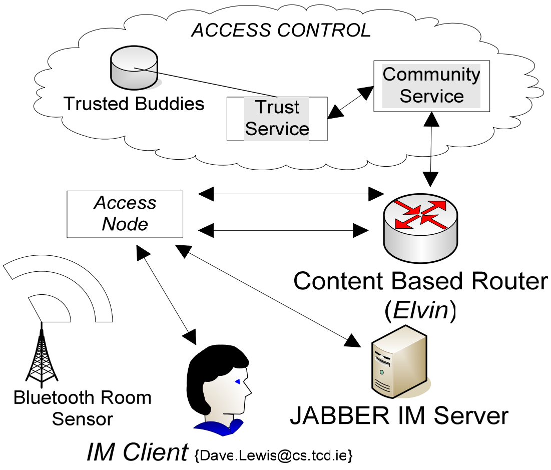

Figure 3. Conference Scenario

1-4244-0143-7/06/$20.00 ©2006 IEEE

As per figure 3 the interactions between the access node and the Access controller over Elvin are presented. There are five actions available; subscription set-up for new user a request location, access node refresh, access control information changes, and subscription deleted as a user is leaving the system. These five actions relate to figure 3 in terms of ‘IM Client’, ‘Access Node’, ‘Elvin’, and ‘Access Control’, respectively.

By way of example we now present the access node refresh action to illustrate the interactions occurring between IM client Access Node, Elvin and Access Control (Community and Trust Service). As per figure 4, the Access Node can request an up-to-date ACCESS CONTROL DECISION for an existing user, by publishing an ACR with an appropriate ID.

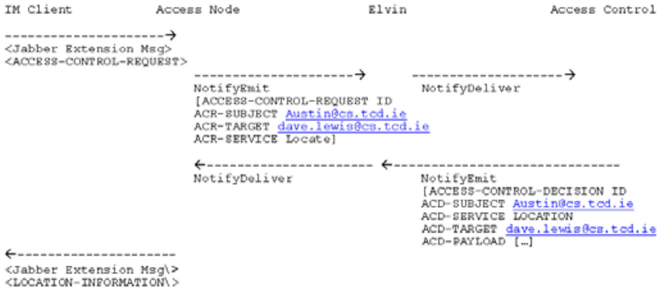

Figure 4. Access Node Refresh

VI. Conclusions & Future Work

This work brought together three pieces of ongoing research by in a novel way by examining how an IM application took advantage of trust and policy information accessed via a decentralized Content Based Network (CBN). The individual research efforts have independent benefits for the overall integrated system. The community work provides limited autonomy, which enables the decentralization of policy management process while still guaranteeing that any high level policies are enforced. The CBN work allows collaborative application information to be pushed to the edge of the network, closer to the user. This is beneficial for reducing access times and bottlenecks when resources expand at an exponential rate. The trust work provides a flexible management mechanism. This is done via a personalized approach and the ability to specify the trust model to many different areas. The collective research work, the overall integrated system, provides its own independent benefits. It provides a generic framework that enables the decentralization and management of collaborative applications such as VoIP and also evolves to reflect peoples changing relationships.

Our next step is to conduct usability experiments on the authoring and management of policies that use the location aware IM application between communities of collaborators. Initially this will focus on management based solely on community based policy management, but this will be followed by usability experiments that combine trust and community based policy management. These evaluations will be based on our ubiquitous computing simulator. CBN related future work will involve further migration of IM-related communications to the CBN. We will also investigate the use of different and more decentralized CBN platforms, e.g. using Siena instead of Elvin. Automatically generating the personalized model of trust on a per user basis is the subject of our ongoing and future work in the area of trust. We envision that this generation will be powered by policy, which will allows the model to adapt as context, risk to date, changes.

Acknowledgment

This work, and Austin Kenny, is supported by the Irish Higher Education Authority under the M-Zones programme. Kevin Feeney is co-funded by an Usher fellowship at TCD. Karl Quinn’s work receives a scholarship from IRCSET.

References

[1] B. Segall, D. Arnold, J. Boot, M. Henderson and T. Phelps, Content Based Routing with Elvin4. CRC for Enterprise Distributed Systems Technology (DSTC), The University of Queensland, St Lucia, 4072 Australia.

[2] P. Saint-Andre “Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence” IETF RFC 3921, The Internet Society, October 2004.

[3] Belokosztolszki, A., Eyers, D.M., Pietzuch, P.R., Bacon, J., Moody, K., "Role-based access control for publish/subscribe middleware architectures". In International Workshop on Distributed Event-Based Systems (DEBS03), ACM SIGMOD, San Diego, CA, USA, 2003. ACM.

[4] Feeney, K., Lewis, D., Wade, V. “Policy-based Management for Internet Communities”, in proc of 5th IEEE International Workshop on Policies and Distributed Systems and Networks (POLICY 2004), IEEE, New York, USA, June 7-9, 2004.

[5] Barrett, R., “People and Policies: Transforming the Human-Computer Partnership”, 5th IEEE International Workshop on Policies and Distributed Systems and Networks, IEEE, 2004.

[6] Feeney, K., Quinn, K., O'Sullivan, D., Lewis, Wade, V.P., 'Relationship-Driven Policy Engineering for Autonomic Organisations', IEEE 6th International Workshop on Policies for Distributed Systems and Networks (POLICY 2005), Stockholm, Sweden, 6-8 June, 2005.

[7] Quinn, K., O'Sullivan, D., Lewis, D., Brennan, R., Wade, V.P., 'deepTrust Management Application for Discovery, Selection, and Composition of Trustworthy Services.' Proceedings of IDIP/IEEE 9th International Symposium on Integrated Network Management (IM 2005), Nice, France, May 2005.

[8] Quinn, K., O'Sullivan, D., Lewis, Wade, V.P., 'Composition of Trustworthy Web Services', Information Technology & Telecommunications Conference, Limerick, Ireland, October ‘04.

[9] O'Neill, E., Klepal, M., Lewis, D., O'Donnell, T., O'Sullivan, D. Pesch, D., ‘A Testbed for Evaluating Human Interaction with Ubiquitous Computing Environments’, In Proceedings 1st International Conference on Testbeds and Research Infrastructures for the DEvelopment of NeTworks and COMmunities (TRIDENCOM'05), Trento (Italy), February 23 - 25, 2005.

[10] Carzaniga, A., Rosenblum, D. S., and Wold, A. L., The Design and Evaluation of a Wide-Area Event Notification Service, ACM Transactions on Computer Systems, Vol. 19, Issue 3, August ’01.

[11] Strom et al., “Gryphon: An Information Flow Based Approach to Message Brokering“, In International Symposium on Software Reliability Engineering 1998.

[12] Chand, R., Antipolis, S., Felber, P., ‘XNET: A Reliable Content-Based Publish/Subscribe System’, Proceedings of the 23rd IEEE International Symposium on Reliable Distributed Systems (SRDS’04), Florianopolis, Brazil, October 18-20, 2004.

1-4244-0143-7/06/$20.00 ©2006 IEEE