ACCESS CONTROL AND JOINT MANAGEMENT FOR COLLABORATIVE PEER GROUPS

Wenhua Qi
School of Electronic and Information Engineering , Beihang University, Xueyuan Rd., Haidian District, Beijing, China

Keywords: Peer groups, Access control, Joint management, JXTA technology.

Abstract: Collaborative peer groups means that multiple self-organizing peers aggregating in a controlled manner to accomplish some collective goals. Peer groups share the properties of peer-to-peer overlay network, including full decentralization, symmetric abilities, and dynamism, which make security problems more complicated. Most prior work focused on authentication, group key management and communication security. However, access control is an important precondition of many security services. Intend for a pure decentralized model without centralized server, our framework employs a distributed delegation authorization mechanism and proposes an authority selection scheme. Multiple authorities could exist in this design, which could avoid single point of failure. Based on the role-based trust management language RT, this paper presents an attribute-based access control framework, and describes a formal joint authorization protocol under voting scheme, to satisfy security requirements of multiple peers. We also introduce our implementation experience by applying JXTA technology.

1 INTRODUCTION

In some cases, multiple self-organizing peers aggregate in a controlled manner, and use multiway communication primitives to accomplish their collective goals. Collaborative peer groups (Sunderam, 2003. Gong, 2002) is introduced to refer to such peer-to-peer networks, which are a strong and flexible structure to enable coordination between applications, server-client, and peers in networks. Group settings may be synchronous or asynchronous manner, and communication models vary from one-to-many or few-to-many to any-to-any.

Collaborative Peer groups share the properties of peer-to-peer overlay network, including full decentralization, symmetric abilities, and dynamism, which make security problems more complicated. Most prior work has been done in the context of group membership authentication, group key management (Rodeh, 2000), and communication security. However, access control is an important precondition of many security services. Conventional group access control mechanisms make authorization decisions based on the identity of requester, such as Gothic (Judge, 2002), Intergroup (Agarwal, 2001). Unfortunately, in distributed environments, members often are unknown to one another; access control based on identity may be ineffective.

Upon the analyses, distributed authorization and access control mechanisms need to be implemented in collaborative peer groups. To avoid single point of failure and enhance scalability of the system, instead of using a centralized model (Judge, 2002), we employ a distributed delegation authorization mechanism and propose an authority selection scheme. Multiple authorities could exist in this design, reducing both the overhead and the response time of group authority. Based on the role-based trust management languages RT (Li, 2002), our work presents an attribute-based access control framework and describes a formal joint authorization protocol under voting scheme, to satisfy security requirements of multiple peers. By applying JXTA technology, we also introduce our implementation architecture and experience.

2 AUTHORITY SELECTION IN PEER GROUPS

Intend for a fully distributed peer group without centralized control over group membership, our framework presents that a peer within the group could

Qi W. (2006).
ACCESS CONTROL AND JOINT MANAGEMENT FOR COLLABORATIVE PEER GROUPS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 83-86
DOI: 10.5220/0002099200830086

propagate its own attributes to other peers. We proposed a quality model based on a set of quality criteria. For each criterion, we provide a definition, indicate its granularity, and provide rules to compute its value for a given peer. Thus, an authority will delegate its authority property to a neighbor which has high quality criteria. This allows the new peers to accept new member into the peer group, reducing both the overhead and the response time of authority.

2.1 Peer Group Quality Model

To differentiate the peers of a group during authority selection, their non-functional properties need to be considered. We consider five generic quality criteria for each peer: (1) cost (2) capacity, (3) age, (4) global trust value, and (5) neighbor link value.

Cost: Given a service to a peer *i*, such as relay service, we define *cost* as the resource cost of a service provider has to pay for providing the service.

Capacity: We define *capacity* as the ability of a peer to process and relay queries and query responses.

Age: We define *age* as the length of time up to now since a peer joins the network up to present.

Trust: We may adopt the trust model EigenRep (Kamvar, 2003) and define *trust* as the global trust value of a peer.

Link: Peers also regularly link to other peers. We define *link* as the number of links from *i* that can reach after at most one indirection.

Given the above quality criteria, the quality vector of a peer *i* is defined as follows.

$Q(i)=(Price_i, Capacity_i, Age_i, Trust_i, Link_i)$

2.2 Authority Selection by Optimization

In our approach, when the group members increase, the authority peer collects information about the QoS of its neighbors, and a quality vector is computed for each of the peers. Based on the quality vectors, a peer with high quality criteria will be selected as the authority peer. This selection process is based on the *weight* assigned by the authority to each criterion, and a set of policy-defined constraints expressed using a simple express language. Examples of constraints that can be expressed include capacity constraints and trust constraints. By merging the quality vectors of all these *n* neighbors, a matrix $Q=(Q_{i,j};\ 1 \le i \le n; 1 \le j \le 5)$ is built, in which each row Q_j corresponds to a peer while each column corresponds to a quality dimension. A Simple Additive Weighting (SAW) (L, 1981) technique is employed to select authority peers in this design, including two phases:

1. Scaling Phase. Some of the criteria could be negative, i.e., the higher the value, the lower the quality, such as Cost. Other criteria are positive, i.e., the higher the value, the higher the quality, such as Capacity. For negative criteria, values are scaled according to $V_{i,j} = \frac{Q_j^{\max} - Q_{i,j}}{Q_j^{\max} - Q_j^{\min}}$. For positive criteria, values are scaled according to $V_{i,j} = \frac{Q_{i,j} - Q_j^{\min}}{Q_j^{\max} - Q_j^{\min}}$.

2. Weighting Phase. The following formula is used to compute the overall quality score for each neighbor:

$$Score(peer_i) = \sum_{j=1}^{5} (V_{i,j} * W_j) \ (0 \le Score(peer_i) \le 1)$$

where $W_j \in [0, 1]$ and $\sum_{j=1}^{5} W_j = 1$. W_j represents the weight of criterion *j*. The authority expresses their preferences regarding QoS by providing values for the weights W_j.

3 JOINT MANAGEMENT

This section presents a role-based trust model and joint authorization protocol to satisfy the access control requirement of peer groups.

3.1 Access Control Policy

In a fully distributed group, our framework adopts credential in trust management (Li, 2002) as authentication method. *Role* is defined as $A.r(h_1, \cdots, h_n)$, where *A* is entity name，*r* is role name. A *Role* may include zero or more restriction parameters h_i. Access Policy has the form of $< r_1 \leftarrow r_2$, vote>, where $r_1 \leftarrow r_2$ is access rule. When a peer requests the role of r_1, the policy statement is checked. *vote* has one of the following forms:

1) true: vote is always true；

2) *fixed(r, m, f)*: A voting is called among members of the *r* role. If *k* votes are received and *f*×*k* are yes, then *vote* is *true*($m, k \in$ integer; $k \ge m; f \in [0,1]$).

3) *dynamic(r, f_1, f_2)*: This is equivalent to *fixed(r,*

$m=n \times f_1, f_2)$, where the role r has n members(m, $k \in$ integer; $f_1, f_2 \in [0,1]$).

3.2 Joint Authorization

The joint authorization protocol based on JXTA technology has five phases, which are *group initialization*, *searching group advertisement*, *authorization request*, *voting*, and *PGC issuance*.

1) Group Initialization. The group authority peer initializes the local secure environment by creating a secure peer group, and then publishes the secure peer group advertisement into the network. The group adv. contains access control policy of peer groups and various parameters such as group name, voting type, etc.

2) Searching Group Advertisement. When a new peer wants to join the group, it must firstly obtain the advertisement of its attributive peer group. In this design peers have two ways to get this information. Peers may discovery the authorization service advertisement from the rendezvous peer or by flooding.

3) Authorization Request. Having the advertisement message, new coming peer may connect with the corresponding authority peer. The new peer will generate a group certificate issuance request containing its desired privileges.

4) Voting. Upon receipt of authorization request, the authority peer first verifies the signature. In a fully distributed peer group, the request is either accepted or rejected by the collective set of current members. The authority peer then propagates the request to call a vote of peers. According to the policy, multiple peers authenticate the attribute of a requester, vote, and reply with a signed message to approve or reject the authorization request.

5) PGC Issuance. Once enough votes are collected, the authority verifies all the votes, and decide whether to accept the new node as a member. If the requester is qualified, the authority will issue the group certificate to it and update the related peer group information. Then, the new node can join the secure peer group.

4 IMPLEMENTATION

We implemented the distributed access control in peer-to-peer collaborative systems using Java programming language. The communication facility among peers is provide by JXTA(Sun, 2002. Altman, 2003), an overlay network middleware messaging system. The measurements are performed on 32 nodes with a high-speed LAN, and each node is the Intel Nocona Xeon 2.8GHz, 2G RAM Linux machine. As the setup phase of the peer group, the Group Authority creates and publishes the group authorization service advertisement. All group access control protocol messages are encapsulated within standard JXTA messages. To satisfy the distributed authorization requirement and balance the group authority overhead, the group authority will republish the authorization service advertisement after delegating the authority attribute to another group member.

The group authorities may receive multi-requests in a short time interval. Figure 1 shows the average join coat for the centralization and delegation. The number of current group members is 30, and the threshold is 30%. In Figure 2 , we plot the accumulated joining ratio against time, and contrast different authorization approaches with 40 new nodes. We can see that after 20 seconds, the success joining ratios vary from 12.5% for a centralized scheme, 50% for two authorities, to 75% for three authorities.

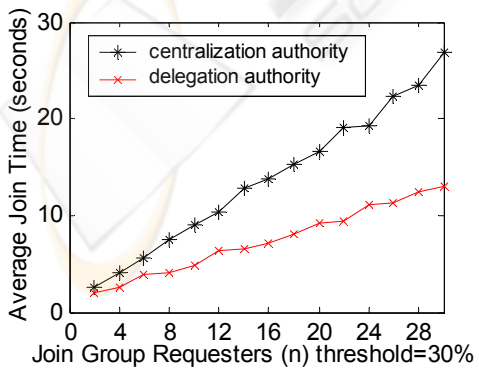

Figure 1: Average Join Cost of Dynamic Requesters.

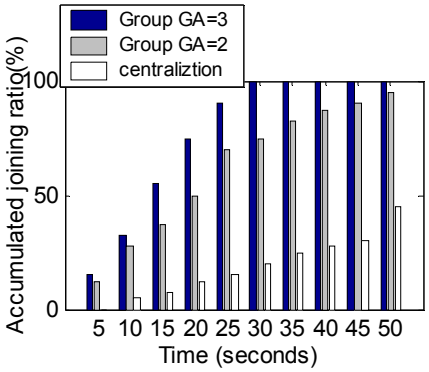

Figure 2: Average Join Cost of Dynamic Requesters.

5 RELATED WORK

Many researches have been accumulated on security in multicast groups. Gothic (Judge, 2002) provides security service for IP-Multicast. An external access control server performs authentication and authorization based on PKI certificates. The Antigone (McDaniel, 1999) utilizes a centralized access control approach in which member access is mediated by a Session Leader.

Sconce(Kim, 2003) presents an admission control framework in peer groups, which treats peer groups as a flat structure where all peer nodes have identical rights and responsibilities. Thus Sconce, which lacks the attribute of peers, can not simplify authorization in collaborative environments. JXTA presents a security mechanism also based on PKI certificates (Altman, 2003). Intergroup (Agarwal, 2001) provides access control by using an authorization service, Akenti (Thompson, 2003), which provides a coarse granularity for access control.

Most of the systems described above provide access control based on identify of participants, instead, this paper adopts attribute-based access control in group. Based on the RT languages (Li, 2002), our work presents a fine-grained access control framework for collaborative peer groups. Meanwhile, based on the policy model, this paper emphasizes the need of joint management for peer groups. Joint authorization efficiently provides security for communication and data resources shared by multiple peers.

6 CONCLUSION

This paper presents a fine-grained and attribute-based access control framework for collaborative peer groups. We propose a distributed delegation authorization mechanism to avoid single point of failure. In order to simplify authorization and access control in collaborations, access control decisions are made based on authenticated attributes of the peers, which improve flexibility of decentralized authorization. By applying JXTA technology, this paper describes a formal joint authorization protocol under voting schemes, to satisfy security requirements of multiple peers.

REFERENCES

Sunderam, V., Pascoe, J., Loader, R., 2003. Towards a Framework for Collaborative Peer Groups. In *the 3rd IEEE/ACM International Symposium on Cluster Computing and the Grid*.

Gong, L., 2002. Project JXTA: A Technology Overview. from http://www.jxta.org/project/www/docs/TechOverview.pdf.

Rodeh, O., Birman, K., Dolev, D., 2000. Using AVL Trees for Fault Tolerant Group Key Management. *Technical Report 2000-1823, Cornell University, Computer Science*.

Judge, P., Ammar, M., 2002. Gothic: A Group Access Control Architecture for Secure Multicast and Anycast. In *INFOCOM*.

Agarwal, D., Chevassut, O., Thompson, M., Tsudik, G., 2001. An Integrated Solution for Secure Group Communication in Wide-Area Networks. In *the 6th IEEE Symposium on Computers and Communications*.

Li, N., Mitchell, J., Winsborough, W., 2002. Design of a Role-Based Trust Management Framework. In *the IEEE Symposium on Security and Privacy*.

Kamvar, S., Schlosser, M., 2003. EigenRep: Reputation Management in P2P Networks. In *the Twelfth International World Wide Web Conference*.

L, H., Yoon, K., 1981. Multiple Criteria Decision Making. *Lecture Notes in Economics and Mathematical Systems*.

Sun Microsystems Project JXTA v2.0: Java Programmer's Guide. 2002, from http://www.jxta.org/.

Altman, J., 2003. Sun Microsystems, Project JXTA: PKI Security for JXTA Overly Networks. from http://www.jxta.org/docs/pki-security-for-jxta.pdf.

McDaniel, P., Prakash, A., Honeyman, P., 1999. Antigone: A Flexible Framework for Secure Group Communication. In *the 8th USENIX Security Symposium*.

Kim, Y., Mazzocchi, D., Tsudik, G., 2003. Admission Control in Peer Groups. In *the IEEE International Symposium on Network Computing and Applications*.

Thompson, M., Essiari, A., Mudumbai, S., 2003. Certificate-Based Authorization Policy in a PKI Environment. *ACM Transactions on Information and System Security*.

Nita-Rotaru, C., Li, N., 2004. A Framework for Role-Based Access Control in Group Communication Systems. In *the International Workshop on Security in Parallel and Distributed Systems*.