[LHK+06] *Nicolas C. Liebau, Oliver Heckmann, Aleksandra Kovacevic, Omid Tafreschi, Markus Fidler, Andreas Mauthe, Ralf Steinmetz;* **A Secure Quorum Based Membership Mechanism for P2P Systems;** 12th Americas Conference on Information Systems (AMCIS 2006), Acapulco, August 2006, S.

A Secure Quorum Based Membership Mechanism for P2P Systems

ABSTRACT

Closed user group based on a Peer-to-Peer system require a membership mechanism that is fully decentralized. Several suggestions have been made in literature. However, the proposed mechanisms have some significant drawbacks since any peer can easily bypass the proposed membership mechanism. In this paper we present a new fully decentralized and scure membership mechanism for Peer-to-Peer systems. A quorum of peers decides about membership requests from new peer. In order to prevent the requesting peer from manipulating the membership decision two mechanisms are applied: (1) The quorum peers must make there membership decision unanimously. This is sufficient to guarantee a correct membership decision, if a fraction of the peers in the P2P system is honest and if the quorum peers are selected in a random manner. (2) In order to ensure a random selection of the quorum peer a random value is created in a distributed way that is used to select the quorum. It can be verified, that the quorum was correctly selected. The presented mechanism is evaluated in terms of the offered security and the created traffic overhead.

Keywords

Peer-to-Peer, Group Membership, Access Control, Quorum-based Decision, Secure Membership

MOTIVATION

The functional spectrum of P2P applications is being much wider than it was initially with high popular file sharing systems. Accordingly, security issues arise with higher intensity and need to be solved respecting the nature of P2P systems. They are highly dynamic systems where members are unpredictable joining and leaving the group. Closed P2P-based user groups that accept new members require a strict membership control without a central trusted third party. Therefore, approaches where several current members of the P2P system vote about the membership of new candidates are applied. Peers in the quorum decide based on defined rules about if membership is granted to a candidate or not.

This solution is not secure if the candidate has the possibility to influence the membership decision. If the number of members that are voting about the candidate is not pre-defined, the candidate could collect as many votes as he has collected the required amount of positive votes to become a member. Even if the number of members that are voting about the candidate is limited, the candidate could try to influence the membership decision e.g. by bribing the voting members. Thus, a membership mechanism must either guarantee that a candidate cannot communicate with the members deciding about the membership, or it must guarantee that the members deciding about the membership are selected randomly. The second solution requires that there is a fraction of honest peers in the system that will never defraud. Further, in order to defeat tries of influencing the voting it requires a unanimous voting result.

This paper presents a secure membership mechanism for closed group Peer-to-Peer (P2P) systems that fulfills all the mentioned requirements. It uses the second alternative to ensure correct membership decision, because in a P2P system it is almost impossible to prevent communication between peers outside the P2P system. The presented mechanism randomizes the quorum selection and makes the selection transparent in order to verify the randomness of the selection.

RELATED WORK

The first effort in this direction was made by Kim, et al. (Yongdae Kim 2003) who developed a group admission control framework based on a menu of cryptographic techniques. This framework classifies the group admission policy according to the entity/ies making the admission decisions, from simple (such as static ACL - Access Control List or attribute-based admission) to the more complex involving fixed external or internal entities. Such simple policies are technically relatively easy to support. However, they are inflexible and not suited for dynamic p2p systems.

As the security problems that arise in P2P networks are overlapping with the one in Ad Hoc networks in general, we considered (Lu 2000), (Kong et al. 2001), (J. Kong 2002) and (Luo et al. 2004; Luo et al. 2002) where a set of protocols for ubiquitous and robust access control in MANETs is proposed. Every member is allowed to participate in access control decisions, thus maintaining the true "peer" nature of ad hoc groups and providing increased availability. Unfortunately, this otherwise elegant scheme has been shown to be insecure (Narasimha et al. 2003), (Jarecki et al. 2004).

Saxena et al. (Saxena et al. 2003) assessed practicality of techniques in (Yongdae Kim 2003). Focus is primarily on performance, but other important features are considered (anonymity, unlinkability and accountability) as well. Their experimental results demonstrated that advanced cryptographic constructs (e.g. threshold signatures) are not yet ready for practical use. However, in (Narasimha et al. 2003) they presented two solutions: one based on so-called threshold RSA signatures - a simple extension of the scheme in (Kong et al. 2001), (Luo et al. 2002) with *verifiability* and another based on threshold DSA signatures that overcomes the problems of the first one.

Recently, Zhang et al. (Y. Zhang 2005) implemented an attribute based access control framework for P2P systems in JXTA. The proposed mechanism is a distributed delegation authorization and decisions are made based on authenticated attributes of the peers in order to achieve flexibility. A voting schema is applied for joint authorization and secure cooperation.

In all these solutions it is still an open issue how to avoid the manipulation of the voting process. We will now present that solves this vulnerability.

A DISTRIBUTED, SECURE P2P MEMBERSHIP SCHEME

This paper presents a membership mechanism for Peer-to-Peer (P2P) systems is presented where the membership decision is made by a quorum, i.e. a set of peers. The quorum is selected in a trustworthy manner. That is, the quorum must be selected in a random manner and it must still be possible to verify that the selection process has not been manipulated or compromised.

Membership Decision

We assume that there are rules defined in the P2P, which peers are allowed to be a member and which not. The decision if a peers is permitted to be a member or not is made by a set of peers, called quorum. In order to make trustworthy decisions it is required that the quorum unanimously approves a membership. That implies that each quorum peer has the possibility of a veto. An obvious drawback is that a peer could use its veto without reason. That is, false negative decisions are possible, however the possibility for false positive decisions is minimized. A false negative decision is equivalent to not following these rules.

In order to make decisions of the presented mechanism more reliable only a subset of trustworthy peers will be allowed to take part in the decisions as quorum member. We will call these peers ***board peers***, as they represent the board of the P2P system. In order to select the board peers we assume a reputation system like (Kamvar et al. 2003), (Wang et al. 2003) to be present in the P2P system. To become a member of the board a peer's reputation must succeed a specific threshold. Board peers that do not follow the membership rules are reported to the reputation system and eventually excluded from the board.

Membership Certificates

Whenever a peer requests to become a member of the P2P system, it has first to contact any peer of the system. This will initialize the membership process. At the end of this process, the requesting peer will either receive a membership certificate if the membership decision was positive, or if not it will receive none. A peer is allowed to apply for membership once every day. The membership certificate serves as proof for the membership and must be presented whenever a peer wants to join the P2P system, i.e. each time the peer comes online. Further, the membership certificate can be used by an access control service to prevent communication of non-member peers to members. The only exception is communication for the membership requests.

Creation of Membership Certificates

To create the membership certificate a document stating the peer's membership status must be signed with a secure key. Requiring only one signature of a single peer would imply that this peer is a central trusted third party that handles all membership requests. This, however, infringes the P2P paradigm. Accordingly, it cannot be assumed that there is a single peer in the system that can be trusted to handle all certificate requests. Therefore, a decision of a group of peers is required in order to avoid, or at least to make it sufficiently hard, that a membership requesting peer can influence the decision. Such a group we call a ***quorum***. To enable a trustworthy decision, we require a unanimous decision of the quorum. This way in case of an attempt to influence the decision, a single honest peer is sufficient to defeat this attempt. To document a positive decision a quorum peer signs the membership request document with its private key. This allows the verification of the quorum composition. This solution requires that each peer possesses a key pair. This could either be issued by a Certification Authority (CA) or a distributed approach like a Web of Trust could be applied. Using a CA seems to infringe the P2P

paradigm. However, an issued key pair will be used by a user for many applications, not only the P2P application. Therefore, we consider that the usage of issued key pairs is an infrastructure mechanism outside P2P systems.

Even with a unanimous quorum decision there is still a security issue if the membership requestor has the opportunity to influence the selection of the quorum peers. This can be avoided if a mechanism can be found that randomizes the quorum selection. As further requirement it must be ex-post possible to verify by any peer, that the process was really randomized and not influenced.

For this reason, we use a distributed mechanism twice in our mechanism. First, a *group of board peers* is used to create a random value in a distributed way. This random value is then used to determine the quorum that has to decide about the membership request and, if granted, has to sign the membership certificate.

PROTOCOL DETAILS

The membership mechanism consist of 5 building blocks: (1) Assigning the board peers, (2) selection of the board peers that administers a specific membership request process, (3) building a list of online board peers, (4) determining the board peers in the quorum by creating a random number using a *group of board peers*, (5) the quorum decides about the membership request based on a unanimous vote and creates the signature under the membership certificate.

Assignment of Board Peers

For our mechanism we assume the existence of two P2P overlay networks (Figure 1). All peers belong to the first overlay network. It is used for all services run over the P2P system apart from the membership service. We call it the *system overlay*. For efficiency reasons there is also a second overlay network comprised of all board peers. We call it *board overlay*. Therefore, board peers have two overlay addresses. The board overlay is organized using a distributed hash table (DHT) like Chord (Stoica et al. 2001), Pastry (Rowstron et al. 2001) or Kademlia (Maymounkov et al. 2002). The DHT is required by the membership mechanism to look up quorum peers in a reliable way. For both overlays we assume a secure peer identification scheme such as the one introduced in (Montenegro et al. 2004), where the peer ID is derived from a peers public key.

Board peers are selected based on the peer's reputation value. If a peer reaches the pre-defined reputation threshold the other board peers will assign an overlay address to the new board peer.

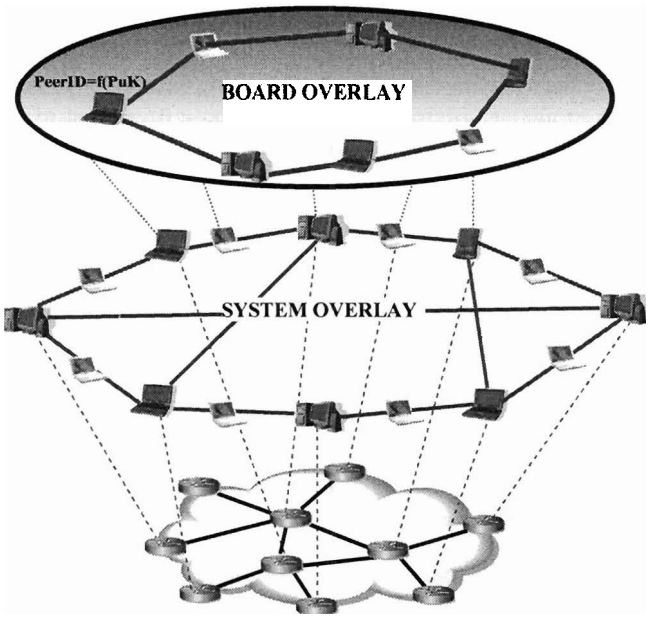

Figure 1. Employed P2P Overlays

Selection of the Board Peer That Administers the Membership Request Process

A membership request can be initially handled by any system peer. The requestor temporarily joins the system overlay and sends a membership request document to the selected peer. The membership request document contains the requestor's

public key, the peer ID of the peer contacted by the requestor and the date of the membership request, as well as information required to decide about the membership. The requestor signs this document with his private key in order to guarantee authentication and integrity. Now the request has to be forwarded to any board peer that will be the administrator for this membership request.

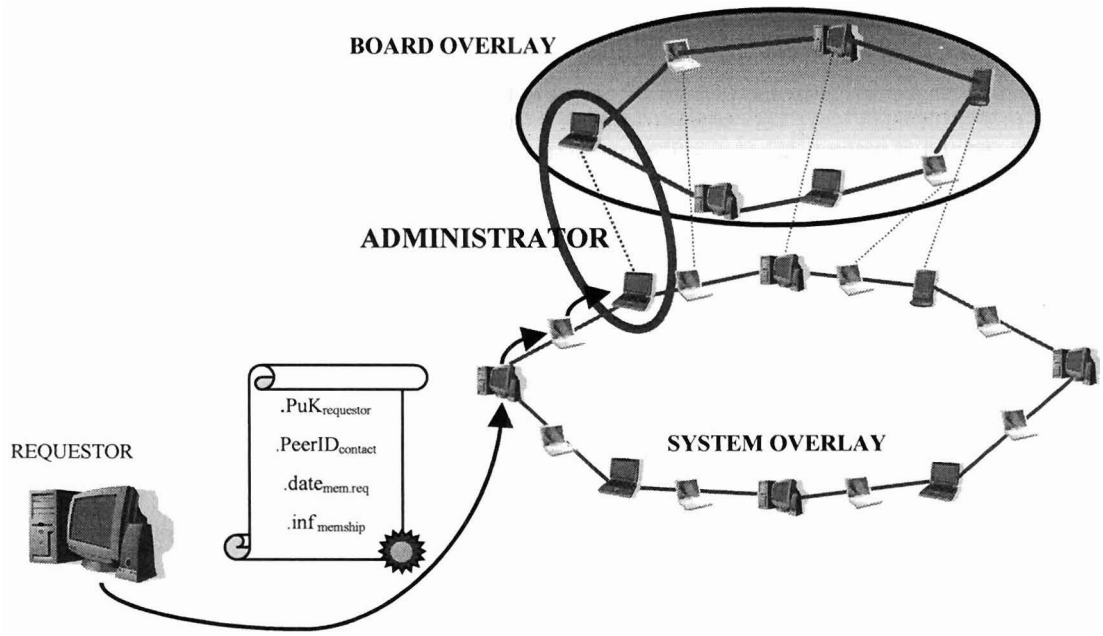

Figure 2. Forwarding the Membership Request to the Administrator

Building the List of Online Board Peers

In P2P systems peers join and leave the system in an unpredictable way. Accordingly, using look up values to determine the responsible peer leads to different results at different times. The purpose of the list of online board peers is to record the status of the board overlay at the moment of the quorum selection to enable ex-post verifying that the correct quorum peers were selected.

To build the list the administrator peer sends a query board overlay. Each board peer receiving the query can now decide if it wants to participate in the membership request process. If it decides to participate it has to guarantee that it will be online for a specific time sufficient to complete the membership request process. It will respond to the query with its board overlay ID. The administrator composes a list with all responses it receives. Naturally, this list maps the whole ID space of the board overlay and can be used to lookup the responsible board peers.

To ensure a random selection of the quorum peers the created list must contain a specific number of peers that is a multiple of the quorum size. Otherwise, the membership process cannot be completed and must be repeated another time.

It is important that the list is being compiled before the group of board peers creates the random value. This way it can be avoided that the result of the list building process is somehow being influenced by a peer that already knows the result of the random value created by the group of board peers.

Creating a Random Value to Determine Board Peers In the Quorum

The responsibility of the group of board peers is to create a random number in a fully distributed fashion that cannot be predetermined. Each peer in the group signs the same document with its private key. The result is a random value at each peer that the other peers cannot predict. These signatures can be combined at the administrator peer to the final random value using for example an XOR-function. This fulfills all requirements. Further, peers want to keeps their own private key secret. Therefore, collaboration of the quorum peers to influence the result of the signatures can be excluded.

The resulting process for creating the random value results in the following: The administrator determines a group of peers. The administrator is absolutely free in the choice of this group. It just has to be k different peers in order to ensure that the value is truly random and cannot be influenced. It forwards the membership request document to all group members. The group members sign the document using their private system key. The signed documents are sent back to the administrator. The administrator combines the signatures to the final random value using the XOR-function.

The final random value is a number of a specific bit length, e.g. 1024 bit long, if RSA based signatures are used. The peer IDs are shorter in length, e.g. 128 bit long. Therefore, the administrator can split the signature into q parts as long as the peer ID. These q numbers will be used by the administrator to lookup the quorum peers that will be responsible for membership decision.

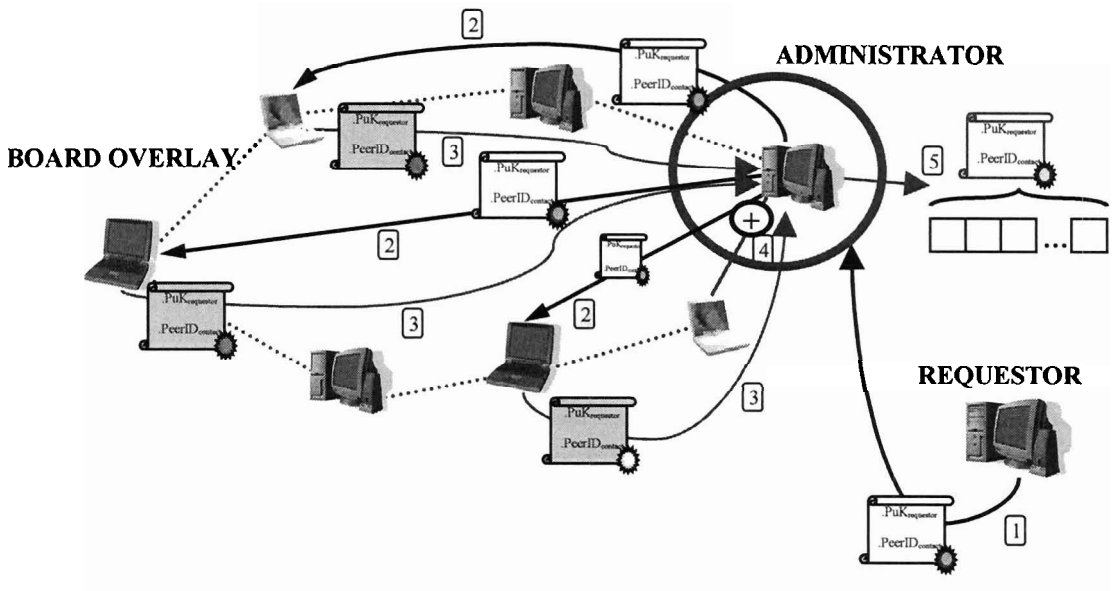

Figure 3: Creating a Random Value to Look Up the Quorum Peers

Membership Decision by the Quorum

The prerequisites for selecting a truly random quorum where it can be proven that the selection was random are now given. There is a list of online board peers (represented through their peer ID) and q random values that can be used as lookup values in the board overlay, where q is the quorum size.

To determine the quorum for each of the q random values a DHT lookup on the list is executed. If a board peer is selected twice, the next board peer in the list is selected instead.

The administrator now adds the list of online board peers to the signed membership request document and sends it to all quorum peers. These will evaluate the membership request according to the rules of the P2P system. If a quorum peer comes to a positive result, it will sign it with its private key (this mean also including the peer's certificate including its public key). Then it will return the signed document to the requestor peer. The requestor peer receives q messages with signed membership certificates. It will copy the parts the quorum peers added (public key and signature) all on one membership certificate. The requestor peer can now use this certificate to join the P2P system and to authenticate itself against other peers.

If a quorum peer concludes that a peer should not be accepted in the P2P system as a member, it reports this to the reputation system together with a report stating the reason. This ensures that a peer cannot apply repeatedly in very short time for membership. Also, this way false decisions can be detected. Board peers making wrong decisions can be detected and their reputation can be decreased in order to finally exclude them from the board peers. Board peers that are not responding to the membership request are also reported to the reputation system and eventually excluded from the board.

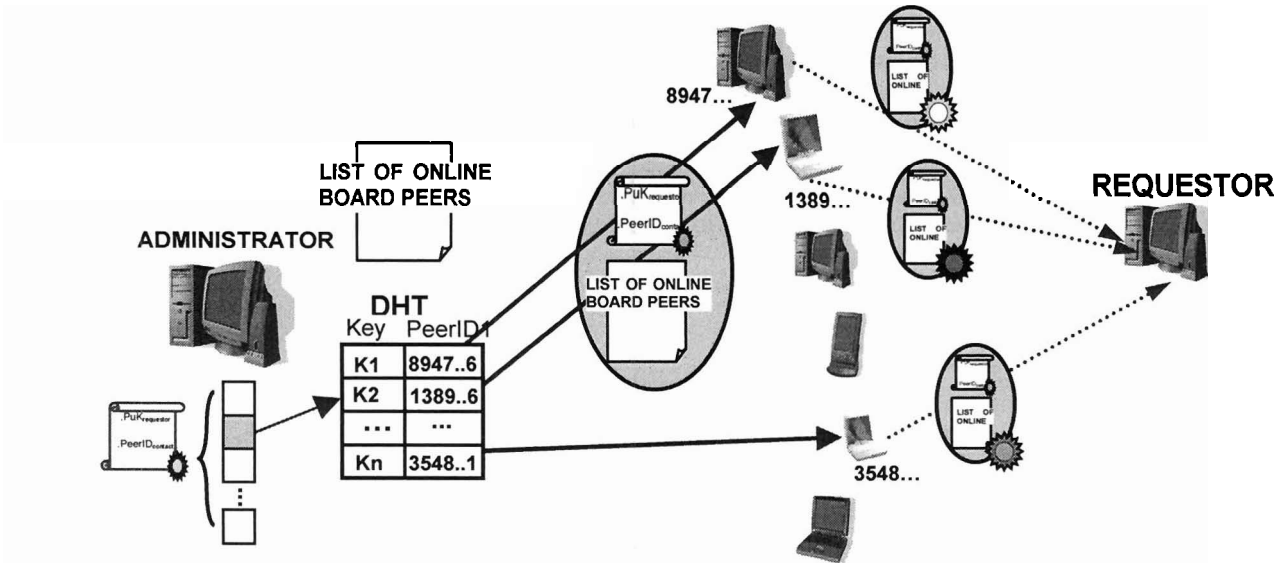

Figure 4: Quorum Selection and Membership Decision

Verifying the Randomness of the Quorum Selection

In the membership credential all information is contained that enables any peer to check if the membership process was executed correctly. That is, each peer can check the signatures in the document that was created by the group of peers. It can compute the random value. A peer has to calculate from the public keys of the quorum peers their peer ID (which is possible due to the use of secure peer IDs) and compare it with the lookup results of the random value (computed from the signatures of the group of board peers) in the board peer list. Finally, all signatures of the quorum peers must verify.

EVALUATION

In order to evaluate if the presented membership mechanism can be applied in practice the two most crucial criteria are scalability and security. First security has to be analyzed as this analysis gives answers to the question which quorum respectively group sizes should be applied. This number influences the scalability.

Security Considerations

We assume a specific percentage of board peers are honest and do not deviate from the membership policy under any circumstances. These peers we call *honest* board peers, where peers willing to defraud the system we call *corrupt* peers.

The security of a membership mechanism is measured by its ability to prevent false positive membership decisions. False positive decision can occur if all peers in the quorum on purpose come to a positive membership decision where it should have been negative. Thus, it is crucial that at least one honest peer belongs to the selected quorum. If there is a specific fraction of honest board peers in the system and the quorum peers are selected randomly, then it can be guaranteed that at least one honest peer belongs to the quorum with a very high probability. This probability depends on the size of the quorum.

Accordingly, the main security mechanism is the random selection of quorum peers. This is independent of the choice of the administrator, as it cannot influence the result of the created random number that determines the quorum.

Quorum Size

If the board peers in the quorum are selected randomly, then the probability of at least one honest board peer in the quorum increases with increasing quorum size. This probability, called the *trustworthiness of the quorum*, can be calculated using Formula 1 (deducted from the hypergeometric distribution):

$$p(T,q,p_g) = 1 - \frac{\binom{T(1-p_g)}{q}}{\binom{T}{q}}$$

T = total number of board peers in the system
q = quorum size
p_g = fraction of honest board peers in the system
$T(1-p_g) \in \mathrm{N}$

Formula 1: Probability for a trustworthy quorum

The resulting required quorum size is depicted in Figure 5.

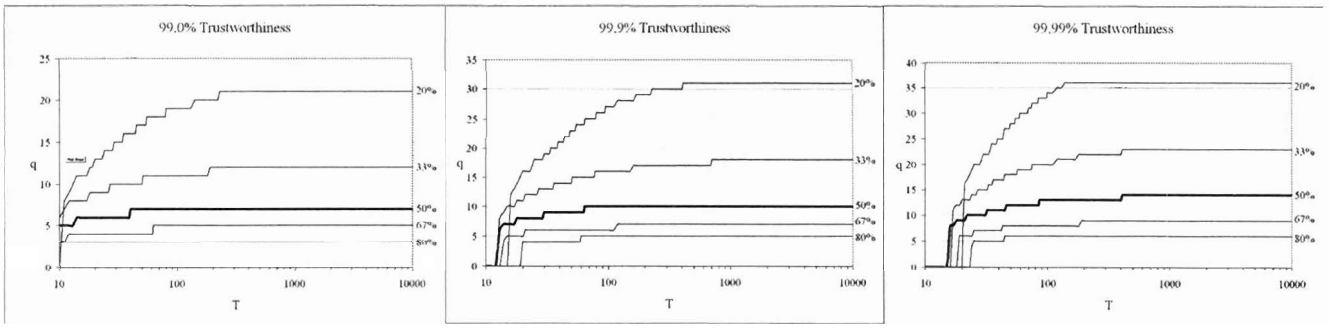

Figure 5: Trustworthiness of a quorum by quorum size, total number of board peers, and percentage of honest board peer

Due to the fact that the board peers are already selected using their reputation value we assume that there are no more than 50% corrupt board peers in the P2P system. Accordingly, for T between 100 and 10000 a quorum size of 14 is sufficient for 99.99% trustworthiness, or a quorum size of 10 is sufficient for a trustworthiness of 99.9%.

With respect to the total number of board peers in the system T it is required to mention, that this is the number of trusted peers that can be chosen from when selecting the quorum. Therefore, T represents just the number of online board peers. When calculating the required quorum size T should be set to the estimated maximum on simultaneously online board peers.

Size of the Group of Boards Peers

The considerations for the quorum can be also applied to the group of board peers that creates the random value for determining the quorum. Nevertheless, here the trustworthiness does not need to be as high as for the quorum. A quorum size of 7 is assumed to be sufficient, as the quorum peers here can hardly influence the result. This would require the knowledge of the private key of the defrauding peers and the modification of the membership request document in a way that the desired random number is the result of the random number generation process. This is computational prohibitive.

Used Signature Scheme and Key Sizes

The random number created by the group of board peers should have a specific length, in order to enable creating q random lookup values. Different options exist for creating this number.

In our system we use RSA based signatures of 1024 bit length. This length is sufficient secure but could be increased. The XOR-value of all signatures of the group of board peers has only a sufficient length for the size of the quorum q of 8 or less. If the quorum is larger, two mechanisms can be applied to circumvent this problem. (1) For lookups in a DHT the most significant bits are the first bits of the lookup values. The last bits often do not influence the lookup result. Because RSA-signatures are not symmetric in their form, the resulting XOR-value can be joined with its backward value (see Figure 6 for an example).

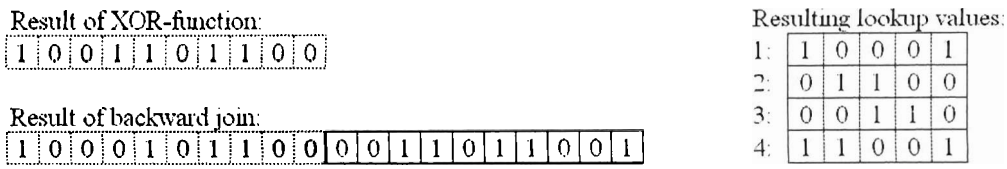

Figure 6: Backwards joining of random number

(2) The second alternative can also be used if the backwards joining does not result in a long enough bit string. Here a sliding window approach is used. As the random value string does not follow any pattern each window over the string delivers a new random value. There are q positions of the sliding window required where the first window is positioned at the start of the string and the last window is positioned at the end of the string. The exact starting position of the i-th sliding window s_i over the string of length l is calculated using (rounded to integer):

$$s_i = i \cdot \frac{l-(r-1)}{q-1}, \quad i \in 0,1,...,q-1$$

Formula 2: Sliding window start position

where r is the required windows size (or required length of the resulting lookup values) and q is the quorum size. An example is shown in Figure 7.

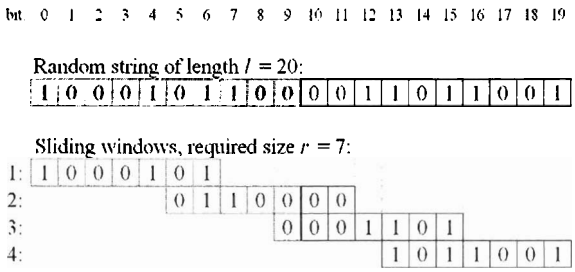

Figure 7: Determining the lookup values using a sliding window for quorum size $q = 4$

Scalability

In the following we present an assessment of the communication overhead of the proposed membership mechanism. The assessment is based on the usage of the JXTA Resolver Service (Microsystems 2004) for message transport. The traffic introduced by the membership mechanism largely depends on the size of the group of board peers and the quorum. We assumed at least 50% of honest board peers in the P2P system. Accordingly, we chose for the group of board peers a size k = 7 and for the quorum a size q = 14. Also we assume a large P2P system with 1000 board peers.

After the administrator received the membership request it builds the list of online board peers. Sending such a query message produces ca. 4,5 Kbytes of upload traffic. Assuming a DHT-based overlay with log(T) fingers the distribution of the query requires ca. 4,5 Mbytes of traffic in the P2P overlay and 56 Kbytes of upload traffic by the administrator. Assuming 50% of all board peers respond to the query the administrator receives 500 messages resulting in ca. 2.7 Mbyte of download traffic to the administrator, again assuming using the JXTA Resolver Service.

Sending the membership request document to the group of board peers creates k messages of 9.5 Kbytes for the administrator. The quorum peers respond with messages of 10 Kbytes. This results in 66.5 Kbytes upload and 70 Kbytes download traffic.

The largest messages being sent during a membership request process are the ones to the quorum and the responses back to the requestor. This is due to the included list of online board peers, for each board peer a peer ID is included. Such a message requires ca. 100 Kbytes of upload traffic for the administrator. Because the administrator has to send q of these messages the administrator has to upload almost 1.4 Mbytes of data. This is clearly the bottleneck of the proposed mechanism, especially as today for most users the upload link has much less bandwidth then the download link. However, for a system with T = 100 the traffic is reduced to 170 Kbytes. Accordingly, the requestor receives ca. 1.4 MByte of data in order to receive all signed membership request documents.

The amount of traffic generated by the number of active board peers T in total and for the upload traffic for administrator is shown in Figure 8, assuming 50% of the online board peers respond to the list query.

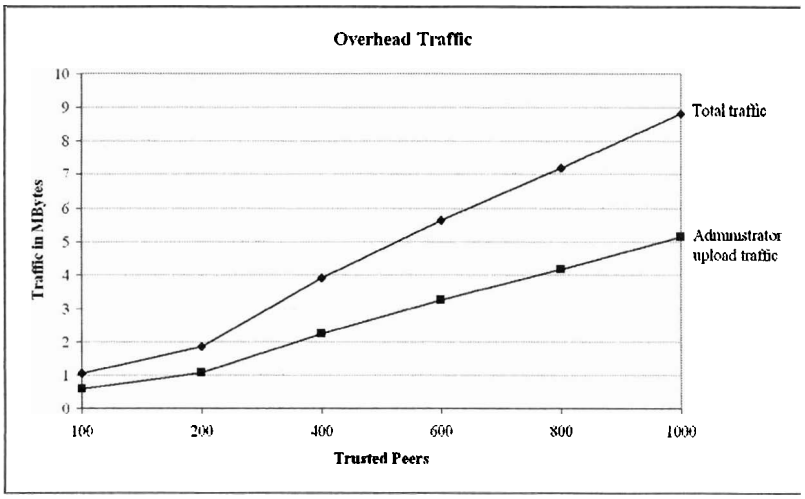

Figure 8: Generated Overhead Traffic

Computational Complexity

The computational complexity of the presented mechanism is moderate per peer. There are a lot of signatures required on the membership certificate, however all the signatures are created in parallel at the quorum peers.

CONCLUSION

A secure membership mechanism for P2P systems was still an open issue. The known solutions offered points of attack that a membership requestor could exploit in order to manipulate the membership decision in his favor. In this paper a novel approach was presented that is comprised of a quorum based membership decision and a mechanism that randomizes the selection of the quorum members in a verifiable way. We assume that a fraction of the peers in the system are honest. Therefore, in order to accept a new peer as a group member it is sufficient, if a quorum that consists of at least one honest peer comes to a unanimous decision. If the quorum peers are selected randomly, it can be guaranteed with a very high probability that at least one honest peer exists in the quorum. In order to select the quorum peers randomly a mechanism is presented that uses signatures of a group of peers to create a random value. This random value cannot be pre-determined. It is used to select the quorum peer. The random value is included in the membership request document to enable verifying that the quorum peers were really selected randomly.

The evaluation showed that a quorum size of 7 to 14 peers is sufficient. Further, it was shown, that the overall traffic per membership request is moderate. A membership request document grows during the process to a size of ca. 100 Kbytes. This is a moderate size. However, the peer administering the membership request has to send and receive over 1.4 Mbytes of data in systems with ca. 1000 board peers. In smaller system the traffic is significantly smaller.

Future work in this area will show, if there are different mechanism that offer the same security properties but can reduce the required traffic significantly.

ACKNOWLEDGMENTS

The authors were supported by the German Federal Ministry of Education and Research under grant 01AK706C, project Premium, and partly supported by the EU FP6 Network of Excellence E-Next (http://www.ist-e-next.net).

REFERENCES

J. KONG, H.L., K. XU, D. L. GU, M. GERLA, AND S. LU "ADAPTIVE SECURITY FOR MULTI-LEVEL AD-HOC NETWORKS," *JOURNAL OF WIRELESS COMMUNICATIONS AND MOBILE COMPUTING (WCMC)* (2) 2002, PP 533–547.

JARECKI, S., SAXENA, N., AND YI, J.H. "AN ATTACK ON THE PROACTIVE RSA SIGNATURE SCHEME IN THE URSA AD HOC NETWORK ACCESS CONTROL PROTOCOL," ACM WORKSHOP ON SECURITY OF AD HOC AND SENSOR NETWORKS (SASN), WASHINGTON, DC, USA, 2004.

KAMVAR, S.D., SCHLOSSER, M.T., AND GARCIA-MOLINA, H. "THE EIGENTRUST ALGORITHM FOR REPUTATION MANAGEMENT IN P2P NETWORKS," WWW '03: PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON WORLD WIDE WEB, BUDAPEST, HUNGARY, 2003, PP. 640-651.

KONG, J., ZERFOS, P., LUO, H., LU, S., AND ZHANG, L. "PROVIDING ROBUST AND UBIQUITOUS SECURITY SUPPORT FOR MOBILE AD-HOC NETWORKS," PROCEEDINGS OF IEEE NINTH INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS (ICNP'01), 2001, PP. 251-260.

LU, H.L.A.S. "UBIQUITOUS AND ROBUST AUTHENTICATION SERVICES FOR AD HOC WIRELESS NETWORKS," DEPT. OF COMPUTER SCIENCE, UCLA.

LUO, H., KONG, J., ZERFOS, P., LU, S., AND ZHANG, L. "URSA: UBIQUITOUS AND ROBUST ACCESS CONTROL FOR MOBILE AD HOC NETWORKS," *IEEE/ACM TRANS. NETW.* (12:6) 2004, PP 1049-1063.

LUO, H., ZERFOS, P., KONG, J., LU, S., AND ZHANG, L. "SELF-SECURING AD HOC WIRELESS NETWORKS," ISCC '02: PROCEEDINGS OF THE SEVENTH INTERNATIONAL SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS (ISCC'02), IEEE COMPUTER SOCIETY, WASHINGTON, DC, USA, 2002, P. 567.

MAYMOUNKOV, P., AND MAZIÉRES, D. "KADEMLIA: A PEER-TO-PEER INFORMATION SYSTEM BASED ON THE XOR METRIC," PROCEEDINGS OF THE 1ST INTERNATIONAL WORKSHOP ON PEER-TO-PEER SYSTEMS (IPTPS02), CAMBRIDGE, USA, 2002.

MICROSYSTEMS, S. "PROJECT JXTA," 2004.

MONTENEGRO, G., AND BAILLY, D. "CRYPTO-ID PROJECT," 2004.

NARASIMHA, M., TSUDIK, G., AND YI, J.H. "ON THE UTILITY OF DISTRIBUTED CRYPTOGRAPHY IN P2P AND MANETS: THE CASE OF MEMBERSHIP CONTROL," ICNP '03: PROCEEDINGS OF THE 11TH IEEE INTERNATIONAL CONFERENCE ON NETWORK PROTOCOLS, IEEE COMPUTER SOCIETY, WASHINGTON, DC, USA, 2003, P. 336.

ROWSTRON, A., AND DRUSCHEL, P. "PASTRY: SCALABLE, DISTRIBUTED OBJECT LOCATION AND ROUTING FOR LARGE-SCALE PEER-TO-PEER SYSTEMS," IFIP/ACM MIDDLEWARE, HEIDELBERG, GERMANY, 2001, PP. 329-350.

SAXENA, N., TSUDIK, G., AND YI, J.H. "ADMISSION CONTROL IN PEER-TO-PEER: DESIGN AND PERFORMANCE EVALUATION," SASN '03: PROCEEDINGS OF THE 1ST ACM WORKSHOP ON SECURITY OF AD HOC AND SENSOR NETWORKS, ACM PRESS, FAIRFAX, VIRGINIA, 2003, PP. 104-113.

STOICA, I., MORRIS, R., KARGER, D., KAASHOEK, M.F., AND BALAKRISHNAN, H. "CHORD: A SCALABLE PEER-TO-PEER LOOKUP SERVICE FOR INTERNET APPLICATIONS," PROCEEDINGS OF THE 2001 CONFERENCE ON APPLICATIONS, TECHNOLOGIES, ARCHITECTURES, AND PROTOCOLS FOR COMPUTER COMMUNICATIONS, ACM PRESS, SAN DIEGO, CALIFORNIA, UNITED STATES, 2001, PP. 149--160.

WANG, Y., AND VASSILEVA, J. "TRUST AND REPUTATION MODEL IN PEER-TO-PEER NETWORKS," 3RD INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING (IEEE P2P 2003), 2003, PP. 150-157.

Y. ZHANG, X.L., J. HUAI "ACCESS CONTROL IN PEER-TO-PEER COLLABORATIVE SYSTEMS," FIRST INTERNATIONAL WORSHOP ON MOBILITY IN PEER-TO-PER SYSTEMS MPPS (ICDCSW '05), IEEE INTERNATIONAL CONFERENCE ON DSTRIBUTED COMPUTING SYSTEMS, 2005.

YONGDAE KIM , D.M., GENE TSUDIK "ADMISSION CONTROL IN PEER GROUPS," PROCEEDINGS OF THE SECOND IEEE INTERNATIONAL SYMPOSIUM ON NETWORK COMPUTING AND APPLICATIONS, 2003, PP. 131 - 139.