Managing group membership in ad hoc m-commerce trading systems

Managing Group Membership in Ad Hoc M-Commerce Trading Systems

Husna Osman and Hamish Taylor
Department of Computer Science,
Heriot-Watt University,
Edinburgh, Scotland. EH14 4AS.
ho12@hw.ac.uk and h.taylor@hw.ac.uk

Abstract—**Managing group membership in an ad hoc m-commerce trading forum is a challenging task as peers may only have partial knowledge of the current membership due to frequent network disconnections, infrequent participation and delays in communication via intermediaries among them. The absence of a centralized network infrastructure adds more complexity to this problem. This paper presents a fully distributed and self-organizing approach to managing group membership in such a loose trading community. It is designed to suit the dynamic nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce.**

Keywords-self-organized group; wireless trading; ad-hoc community; peer-to-peer

I. INTRODUCTION

A basic concept in ad hoc m-commerce trading systems is the formation of a trading forum by two or more peers that are in the vicinity of each other and run an appropriate software application. This trading forum defines the rules of trading and provides the context for mobile users to engage in mobile commerce using ad hoc wireless networking [1]. It is a self-organized and self-configured m-commerce domain that can be initiated by any peer with suitable networking capability and does not require any centralized infrastructure to manage it. Its participants communicate and cooperate with each other by utilizing their local resources and also their neighbours' to accomplish the following tasks:-

1) Engage in ad hoc m-commerce transactions such as swapping of digital resources, buying or selling items, mobile auctions, consortium trading and so on [1].
2) Give recommendations about other members' identities, trading histories and reputations.
3) Attest other members' digital certificates that bind together their identity information with their public keys.
4) Evaluate each other by providing deal evaluations of transactions.
5) Share negative evaluations about their trading partners with other members in the forum.
6) Sanction those members who misbehave or have a history of being given poor evaluations of their trades.

As an example, a group of peers with wireless networking capability and a mobile auction application installed on each device comes into communication range with each other. One of the peers reestablishes a trading forum that offers auction services and advertises it for other peers with similar interests to join. Peers able to join the trading forum session can then participate in the auction activities as sellers or bidders. The mobile auction application that runs on each peer's device handles all the auction processes and provides a graphical interface to the users. After the completion of each transaction, peers can provide deal evaluations to each other. Positive evaluations will increase a peer's reputation and thus increase other peers' trust and willingness to trade with that party in future transactions, while negative evaluations reduce other peers' confidence to transact with the peer and open that peer to the risk of sanctions from its trading forum.

One of the major security concerns in such trading systems is to establish sufficient trust among participating parties in a trading forum in order to mitigate the uncertainty and risks involved in its transactions. While some trading forums will choose to remain open to all comers, others will choose to use membership as a means for establishing greater trust and more secure interactions among its group members. As new parties may apply to join and existing members may have to be excluded, the management and maintenance of such trading forums entails support for a service to handle group membership.

The function of a group membership service is to track membership changes in a trading forum and help determine whether a peer is currently a member of a particular trading forum [2]. It consists of mechanisms for peers to join and be excluded from the trading forum, as well as to verify membership. However, to manage group membership in such a loose ad hoc m-commerce community with frequent and unpredictable network disconnections, infrequent communication among group members and in the absence of a centralized network infrastructure is a challenging task as each member cannot be expected to have a complete or mutually compatible view of group membership.

Hence, this paper proposes a fully distributed and self-organizing approach for managing group membership in ad hoc m-commerce trading forums, which is based on membership vouchers, quorate decisions by some group

members, partial membership lists and the use of digital signatures.

The rest of this paper is organized as follows. Section II describes solution requirements and assumptions. Section III gives a brief overview of related work. Section IV presents the details of each mechanism in our approach. Section V demonstrates a number of reference scenarios and finally, Section VI concludes the paper.

II. REQUIREMENTS AND ASSUMPTIONS

Due to the challenges posed by the nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce [1], the following requirements for managing a trading forum's group membership will be needed on top of the usual requirements for interactive m-commerce software such as adequate quality of service and reliability in the wireless network, end-to-end security and so on:

1) Resource-limited
The processes and operating costs of group membership management should be affordable for resource-constrained devices.

2) Dynamic
Group membership management should be able to handle dynamic membership changes without having to reconstitute the group.

3) Absence of Authority
The responsibility for managing the group membership has to be devolved among members without recourse to trusted parties with delegated authority as the presence of no party can be guaranteed in any live trading context.

4) Robustness
Intermittent participation by members, unreliable means of communication and the absence of dependable enduring infrastructure services requires failure tolerance throughout support for system services.

5) Convenience
The management of group membership should not involve users in complicated and time consuming activities nor should making changes in membership status take very long periods.

We assume that support for group members' identity establishment and verification is provided by a security and trust service. Details and discussion of this are part of ongoing work and will be published later. We illustrate in Fig. 1 below an abstract architecture for each trading peer in an ad hoc m-commerce trading forum. The first two layers sequentially include a mobile device and an operating system required for operating the applications. The Service layer provides services that are required to support the core functionality of the trading system which include the following:

- Discovery Service
  Provides the ability for peers to search and discover available trading forums, advertisements and other peers in the network.

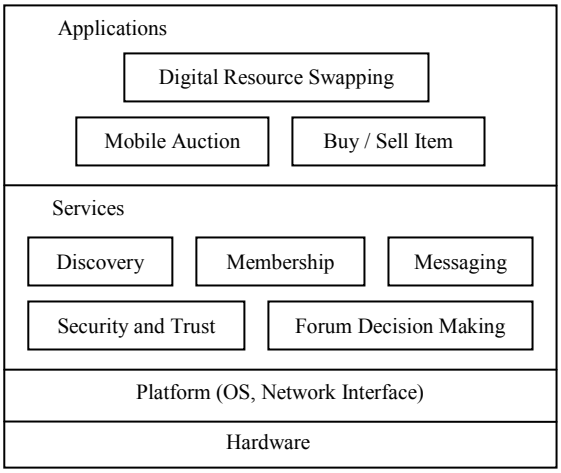

Figure 1. An abstract architecture for an ad hoc m-commerce trading peer.

- Membership Service
  Provides the ability for peers to organize themselves into a trading forum, which includes the ability to join, renew membership and also to exclude a member from a trading forum.

- Forum Decision Making Service
  To facilitate any decision making processes by fostering effective communication among forum members.

- Messaging Service
  Provides support for message delivery over the network. This includes specifications for routing, relaying and propagating messages as well as the message structure and so on.

- Security and Trust Service
  Provides support for identity establishment, trust establishment as well as message authentication, integrity, confidentiality and non-repudiation. This service will also provide security advice to make participating users understand the issues and their responsibilities in securing ad hoc m-commerce trading systems.

The Application layer is the implementation of ad hoc m-commerce applications such as mobile auctions, swapping of digital resources, buying or selling items and so on.

III. RELATED WORK

Several relevant papers have been published in the area of group membership in ad hoc wireless networks such as [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16]. The main focus of most of the work is to provide secure communications among group members, in which some of the solutions proposed are based on group key agreements. Maki, Aura and Hietalahi in [5] have proposed a distributed certificate-based system to establish secure communications among members in ad hoc groups, where a certificate that is signed by a group key is used to indicate the membership of each member. The group key is used as the identifier of the group and is generated by a group leader who is responsible for managing the group

membership. To avoid a single point of failure, a group leader's authority is distributed to multiple sub-leaders. Thus, a group can have one or more group leaders or sub-leaders. A similar approach is used by Steiner, Tsudik and Waidner in [6] to address the issue of secure group communications in dynamic peer groups. They have proposed a protocol called CLIQUES which is based on a multiparty extension of Diffie-Hellman key exchange. In this protocol, all members contribute to the establishment of a group key. Whenever there is a membership change, the group key is reconstructed. This approach also depends on having a group controller to manage the group membership. Liu, Sacchetti, Sailhan and Issarny [13] in their design of a generic group management service for mobile ad hoc networks (MANET) have also proposed a group leader for managing the group dynamics. In their approach, the group leader's role is rotated from one member to another in order to distribute the load of group management among members and also to address the issue of group leaders dropping out of participation. The selection of the group leader is based on a number of criteria that have been defined [13].

Another approach is a virtual partitioning (VP) based group membership algorithm by Pradan and Helal [10]. This approach requires each group member to maintain a complete and consistent view of group membership. Roman, Huang and Hazemi in [4] have also proposed an algorithm to maintain a consistent view of group membership in ad hoc wireless networks based on location information.

Group key agreement does not seem to be workable for ad hoc m-commerce trading forums. Participation by all members on a regular and frequent basis would be required in order that new group keys could be constructed in a timely way for each membership change and also for each member to get access to the new group keys every time they are reconstructed. However, casual local online trading is likely to involve a mixture of frequent and infrequent participants and quite an amount of irregular participation. Thus, it may not be possible for a new group key to be constructed in a timely way for each membership change on each occasion that requires contribution by all group members. It will take unpredictable periods of time for all members to be available for the reconstruction process to happen. This might delay the first opportunity for a new member to participate in the group communications as well as other activities of the trading forum. This might also give an opportunity for a member subject to exclusion proceedings to remain as a member for a longer period of time. On other occasions, the unavailability of some members during the reconstruction of the group key might cause them to be unable to get access to the new group key and thus might lead to the group shrinking as a subset of the members reconstruct the group key among themselves. The reacceptance of these unavailable members in the trading forum would demand the group key be reconstructed again. This might lead to endless reconstruction of group keys as frequent and regular participation by all group members cannot be guaranteed in ad hoc m-commerce trading forums.

A hierarchical structure where one or more group leaders are responsible for managing the group membership also does not seem to be workable for our work as the presence of such authority in the current group context cannot be guaranteed all the time. Furthermore, the loose nature of relationships in casual local trading networks does not support the assumption of a core of well trusted parties around which the rest of the trading community is constituted. Thus, a flat structure where all members are given equal responsibility to manage the group membership would seem to be more appropriate.

The requirement for each member to maintain a complete and consistent view of current group membership is also not realistic for ad hoc m-commerce trading forums. Communication among members will often involve intermediaries, be subject to frequent disconnections and take unpredictable periods of time from minutes to several days or weeks with infrequent participants. Getting all group members to participate in every membership decision will take too long to be practical. So membership decision making needs to be delegated to subsets of the membership and other members will have to accept their decision making when it is eventually communicated to them. That in turn means that every member will only have a partial view of the membership.

IV. APPROACH

In this section, we describe our approach for managing group membership in ad hoc m-commerce trading forums.

A. Membership Voucher

A membership voucher serves as a credential that can be used by forum members to prove their membership to other members of the forum. It contains the following information as a minimum:-

- The trading forum name and ID.
- Its holder's trading pseudonym or ID.
- The collection of approvals and any vetoes among verified votes. Each vote will consists of the voter's trading pseudonym or ID, the subject of the vote either a joining request or membership renewal request, the requestor's trading pseudonym or ID, voter's agree or disagree statement, time and date as well as the digital signature of the voter.
- Digital signature of its issuer.
- A validity period.

To be recognised as a member of a trading forum, each peer must possess a membership voucher that is digitally signed by other group members who are expected to be recognised. A recognised member is a member whose membership voucher has been verified as having the following:-

- Its validity period has not expired.
- Has been issued and signed by parties who are recognised as members at the time the membership voucher is issued.

- Has sufficient number of votes from parties who are recognised as members at the time they participated in the vote.

Peers present the voucher and their certificate to attest their membership and receiving peers use the resources available to them such as personal records of previously known members of the forum to decide whether to accept the claim. Members exchange these records with other trusted members to widen and update their views of the scope of membership. However, as the judgments are made independently by each peer based on their partial membership views without involving any authority higher than a peer, membership claims cannot always be settled to the satisfaction of all reasonable peers. It will depend on the level of trust that the receiving peers have in the issuer and the voters of the presenting peers' membership voucher as well as the parties that attest their membership vouchers. If the receiving peers trust those parties, it is expected that they will accept the presenting peer's membership claim.

The validity period of the voucher is used as a regular way to review the membership status of each member. After its expiry date has elapsed, the voucher is no longer applicable to prove a peer's membership. Thus, to remain as a current member of a particular trading forum, each peer needs periodically to renew their membership voucher when the existing voucher expires.

B. Quorate Decisions

As members of a trading forum are peers that have similar constraints on their devices and are offline most of the time, it is not realistic to expect to have a trusted peer or unbroken chain of trusted peers to be responsible for managing the group membership that is reachable all the time. All peers are given equal responsibility in order to avoid circumstances where decisions cannot be made due to the unavailability of an appropriate authority. Therefore, in this work, the decisions to accept new members, exclude misbehaving members and also renew existing members' membership vouchers are distributed to any sufficiently large subset of existing group members. How many members need to agree and the maximum number of members allowed to disagree in order to elicit a quorate decision will depend on each trading forum's decision making policies.

A trading forum's decision making policy can be made simpler or more stringent depending on the type of ad hoc m-commerce trading. A simple policy is probably more desirable for circumstances that entail fast decision making, such as in the admission process. It may require only a small number of approval replies and no vetoes. For example, a trading forum with 30 current members may require only a small fraction of currently active and connected members to agree and none to disagree, in order to obtain a quorate decision whether to accept or reject the application of a new member. By having such a policy, new admissions could take place rapidly. On the other hand, to obtain a quorate decision for a more stringent decision making policy might require a definite higher number of approvals and less than a threshold number of vetoes. This may involve currently offline members as the replies from currently connected members may not be sufficient to obtain a quorate decision. However, to elicit the required number of members' votes may take some time as many members may not be reachable for significant periods or may not participate frequently in group communications. Thus, this type of policy might be more appropriate for circumstances that do not require rapid decision making such as in the membership renewal process or exclusion of members, which require more careful consideration. For example, to exclude a member from a trading forum of 40 current members might require at least 20 members to agree and less than 5 members disagree with the exclusion proposal.

C. Membership Lists

A membership list contains records about sometime members of a trading forum. It also provides information about the status of each member as to whether a member is a current member or former member or has been excluded. A complete membership list would keep members updated with the current membership of a particular group [10].

However, all members of an ad hoc m-commerce trading forum cannot be expected to have a complete and consistent view of membership as some of them may be offline or unreachable or may not participate in group communications regularly or may be active but not yet have had messages passed on to them about decisions taken by other members. Instead, members of an ad hoc m-commerce trading forum will each maintain a partial list of members and exclusions that they know about and accept in their local storage and exchange it with other members to update and widen their view of membership every time they participate in the trading forum.

D. Digital Signature

A digital signature is used to guarantee the authenticity and integrity of a message or document sent by a peer as well as to ensure that the sender cannot get away with denying having sent the message or document. In ad hoc m-commerce trading forums, messages and documents such as membership requests, votes, membership vouchers, exclusion proposals and also exclusion orders are digitally signed by their sender in order to give assurance to the receiving peers that those messages or documents were actually sent by the specified sender and were not altered during transmission and also so that the sender will not be able to credibly deny having sent the message.

E. Join Mechanism

For a new member to join a trading forum, he must first discover a member of the forum and then send a join request. The following steps are involved:-

1) Sending a request to join

A new member (M_{new}) sends a join request message together with his digital certificate to at least one member of the trading forum. The certificate must be self-signed but may also be signed by other parties. The join request message will contain the following information as a minimum:-

- The target trading forum name and ID
- M_{new}'s trading pseudonym or ID
- Digital signature of M_{new}

2) Propagate Join Request

Upon receiving the join request message, the contacted member ($M_{contact}$) will then propagate it to other members of the forum in order to obtain a quorate decision whether to accept or reject the application. The propagated message will have a time limit (TTL) in order to limit the voting period. However, $M_{contact}$ may consider having extra rounds of voting if the verified votes received are not sufficient to obtain a quorate decision after the voting period limit has expired.

3) Quorate decision by other members

Other members of the forum with views on the proposal are then expected to reply with either a signed agree or disagree message to $M_{contact}$, accompanied by their membership voucher as a proof of their membership.

4) Issuance of membership voucher

Upon receiving the replies, $M_{contact}$ will verify the voters' membership vouchers as not having expired and as being of members $M_{contact}$ recognises as members or having sufficient signatures of parties $M_{contact}$ recognises as members at the time the membership vouchers were issued. Fig. 2 below depicts the steps involved in the verification process. Votes that are not verified or are received after the time limit are discarded. Then the forum's admissions policy is applied to the verified votes. If there are sufficient acceptances and less than sufficient vetoes, $M_{contact}$ will send a signed standard membership voucher to M_{new}. In addition to a membership voucher, $M_{contact}$ will also send his local partial lists of known members and known members to be excluded to M_{new}.

5) Update membership list

M_{new} will then notify other members about his new membership by multicasting a Hello message accompanied by his membership voucher to all currently active and connected members of the group. They will pass the multicast on during further group interactions until the multicast message's liveness expires.

F. Exclusion Mechanism

To induce participating parties in ad hoc m-commerce trading systems to act honestly and in a trustworthy way, it is valuable to have a mechanism to sanction forum members that misbehave or have a history of being given poor evaluations of their trades. One of the appropriate ways to do this is exclusion from membership. By having a mechanism to exclude misbehaving members, a group membership service can provide a degree of assurance about forum members' trustworthiness and reputations. It will sit alongside the reputation system, which is one of the elements in our security and trust service, and serves as the primary service to help assess the behavior and also the trustworthiness of each member.

Similar to the join process, to exclude an existing member requires a quorate decision from other members of the trading forum. The following steps involved:-

Upon receiving the votes, $M_{contact}$ will execute the following algorithm:-

```
Check whether the validity period of the voter's membership voucher is still applicable
If yes
  Check whether the voter is a recognised member in his membership lists
  If yes
    Accept vote
  Else
    Check whether the voter's membership voucher is issued and signed by a recognised member at the time it is issued and has sufficient votes from recognised members at the time they participated in the vote
    If yes
      Accept vote
    Else
      Check whether the membership voucher of the unrecognised issuer and voters are issued and signed by a recognised member at the time it is issued and has sufficient votes from recognised members at the time they participated in the vote
      If yes
        Accept vote
      Else
        Discard vote
Else
    Discard Vote
```

Figure 2. Voter's membership voucher verification steps.

1) Multicasting a proposal to exclude

An existing member ($M_{propose}$) can propose to exclude a misbehaving member or a member with poor evaluations from a trading forum by multicasting a proposal to exclude message to other forum members except the target member (M_{target}). The message will consist of the following information:-

- The target member's ID or trading pseudonym.
- $M_{propose}$ digital signature

In addition to that, an accompanying note giving brief reasons for the exclusion might also be expected.

2) Quorate decision by other members

If other forum members agree or disagree with the exclusion proposal, they will reply with a signed agree or disagree message to $M_{propose}$ within the required time period. The message will consist of similar contents as in the votes for joining and membership renewal request as mentioned in section IV (A) above, except that the message subject will be the exclusion proposal. In addition to that, the trading pseudonym or ID of the proposed member to be excluded will also be included in the message.

3) Multicasting an exclusion order

Once enough replies from validated members are collected within the voting time period limit and the forum's exclusion criteria are satisfied, $M_{propose}$ will then multicast an exclusion order to other currently connected members. The exclusion order will have the following details:-

- The target's trading pseudonym or ID
- The collection of signed messages approving and disapproving the target's exclusion.
- Digital signature of $M_{propose}$.
- Exclusion period

In this case, forum members are expected to refrain from issuing a new membership voucher to the target member after the validity period of his current membership voucher has expired until the exclusion period has ended. Also, any votes or membership vouchers issued by the target member will not be considered as valid. Furthermore, forum members are also expected to not participate in any transactions with that member.

G. Membership Renewal Mechanism

To remain as a member of a trading forum, each member should renew their membership near the end or after the validity period of their current membership voucher expires. The following steps are involved:-

1) Sending a membership renewal request

A member who holds an expired or soon to expire membership voucher sends a membership renewal request together with his old or current membership voucher to at least one of the current members of the trading forum ($M_{contact}$).

2) Propagate Renewal Request

Similar to the join and exclusion mechanisms, to renew a membership voucher also requires a quorate decision from other forum members. Thus, upon receiving the membership renewal request, $M_{contact}$ will then propagate it to other forum members in order to obtain a quorate decision whether to accept or reject the renewal request.

3) Quorate decision by other members

In this situation, other members are expected to check whether any non-expired order has been issued to exclude the requesting member from the trading forum before they each reply with either a digitally signed agree or disagree message together with their valid membership voucher to $M_{contact}$.

4)Collate agree messages

Once enough replies from validated members are collected within the voting period limit and the forum's membership renewal criteria are satisfied, $M_{contact}$ then collates the replies and sends them together with a new membership voucher to the requesting member. The voucher is signed by $M_{contact}$ as an accurate record of the vote.

H. Message Propagation

In this work, each message is associated with a unique identifier and a time to live (TTL). To ensure reliable message propagation, each time a peer receives a message for the first time, it will accept the message, store it and also forward it once to each of its directly connected neighbours except the sender during the period of its lifetime. To prevent duplicate propagation, each time a peer receives the same message more than once, the message will be discarded. As all of the mechanisms discussed above require sufficient members' votes to obtain a quorate decision, it is important for each voting activity to have an expiry time. Therefore, the use of a TTL will ensure that each propagated message is discarded after its time limit has expired.

V. Reference Scenarios

We demonstrate each of the above mechanisms in a series of scenarios below.

A. Scenario 1 – Joining

A trading forum A consists of 5 members M_1, M_2, M_3, M_4 and M_5. All members are online during communication period t_1. It is assumed that:-

- Each of them possesses a current membership voucher
- Each member's local membership list contains the membership records of other members as follows:
  M_1 (M_2, M_3, M_4, M_5)
  M_2 (M_1, M_3, M_4, M_5)
  M_3 (M_1, M_2, M_4, M_5)
  M_4 (M_1, M_2, M_3, M_5)
  M_5 (M_1, M_2, M_3, M_4)
- No member has any knowledge of parties to be excluded.
- This trading forum applies a simple admissions policy that requires at least three members agree with the new application and none disagrees while votes are being gathered.

A new member M_6 comes into their communication range and sends a join request to M_2 together with his self-signed digital certificate. M_2 then propagates the request to other members. It is assumed that all members agree to accept the new application from M_6. They then each reply to M_2 with their digitally signed agree message together with their membership voucher. Upon receiving the replies, M_2 will then verify each of the voters' membership vouchers. In this case, all votes are accepted as each of the voters possesses a current membership voucher and M_2 recognises them all as members in his membership lists. M_2 then applies the trading forum's admissions policy to the verified votes and sends a signed standard membership voucher containing the four signed approvals and its local membership list to M_6. M_6 then sends a hello message together with his membership voucher to other connected members in order to notify them of his new membership. Upon receiving M_6's hello message and membership voucher, other connected members will independently verify M_6's membership voucher before accepting the new membership and update their local membership list. This scenario is illustrated in Fig. 3 below. At the end of communication period t_1, the local membership list of each member will be as follows:-

M_1 (M_2, M_3, M_4, M_5, M_6)
M_2 (M_1, M_3, M_4, M_5, M_6)
M_3 (M_1, M_2, M_4, M_5, M_6)
M_4 (M_1, M_2, M_3, M_5, M_6)
M_5 (M_1, M_2, M_3, M_4, M_6)
M_6 (M_1, M_2, M_3, M_4, M_5)

B. Scenario 2 – Exclusion

This scenario takes place after the earlier one. It is assumed that:

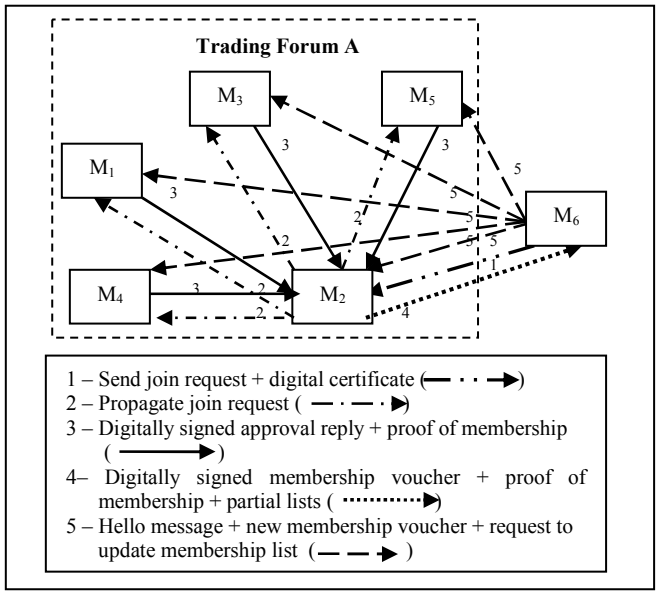

Figure 3. A join scenario with five members (all online).

- During this communication period, trading forum A consists of 20 parties (M_1, M_2, ……, M_{19} and M_{20}) that possess a current membership voucher. However, only M_1, M_2, M_3, M_4, M_8, M_{10}, M_{15}, M_{16}, M_{17} and M_{19} are online while the others have gone offline.
- This trading forum applies an exclusion policy that requires at least 7 members to agree with the exclusion and less than 3 vetoes before any member can be excluded.
- The local membership list of each currently connected member contains the membership record of other connected members as each of them needs to send a hello message together with their membership voucher to all connected members in order to rejoin the trading forum after being offline or disconnected from the network.

M_2 multicasts a proposal to exclude M_8 to all currently connected members of the forum except M_8. It is assumed that all reply and only M_1, M_3, M_4, M_{10}, M_{15} and M_{19} agree with the exclusion proposal while the others disagree, and M_2 receives their digitally signed votes within the voting period limit. Upon receiving the votes, M_2 then verifies the voters' membership voucher and accepts their votes as the validity period on their membership vouchers are still applicable and M_2 recognises them all as members in his local membership list. After adding his own approval vote and the forum's exclusion policy is applied, there are sufficient number of approvals (7 approvals) and less than sufficient vetoes (2 vetoes) for M_2 to obtain a quorate decision to issue an exclusion order. M_2 then multicasts the exclusion order to all connected members except M_8. This scenario is illustrated in Fig. 4 below.

C. Scenario 3 - Renewal

In this scenario, trading forum A consists of 25 current members (M_1, M_2, ….M_7, M_9, ……, M_{25}) and it is assumed that:

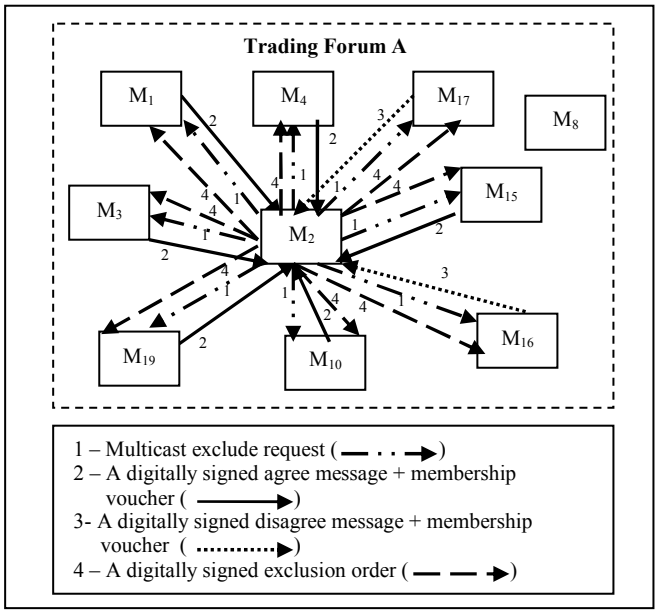

Figure 4. An exclusion scenario

- In the beginning, only M_1, M_4, M_6, M_7, M_9 and M_{10} are online while the others are offline.
- M_1's membership voucher is nearly expired.
- Renewal policy requires at least 7 members to agree with the renewal request and no vetoes before any new membership voucher can be issued to the requesting member.

M_1 sends a membership renewal request together with his current membership voucher to M_9 who then propagates the request to other currently connected members. It is assumed that only M_4, M_6 and M_7 agree with the request and reply with a digitally signed agree message together with their membership voucher to M_9 as depicted in Fig. 5 below. It is assumed that M_{10} received the propagated message but decided not to participate in the vote. Upon receiving the agree replies, M_9 then verifies M_4, M_6 and M_7s' membership vouchers and accepts their votes as the validity period on their membership voucher is still applicable and M_9 recognises them as members in his local membership list. However, in this situation, the number of approval replies is still not sufficient for M_9 to obtain a quorate decision to issue a new membership voucher to M_1. Thus, M_9 has to wait until the voting period limit expires before he can consider a second round of voting.

After some further time has elapsed within the same voting period limit, it is assumed that M_4, M_6, M_7 and M_{10} have gone offline while M_2, M_5, M_{20}, M_{23}, and M_{25} come into communication range with M_1 and M_9. The others remain offline. M_9 then propagates the membership renewal request to M_2, M_5, M_{20}, and M_{23} after receiving their Hello Message and verifies their membership voucher. In this case, it is assumed that M_9 did not accept M_{25}'s membership claim as he did not recognise either the issuer of M_{25}'s membership voucher or the issuer and voters of that issuer as members in his membership list. Thus, the renewal request is not propagated

to M_{25}. M_2, M_5, M_{20}, and M_{23} agree with the request and they each reply with a digitally signed agree message together with their membership voucher to M_9 within the voting period limit. M_9 then validates their votes. Validated votes from M_2, M_5, M_{20}, and M_{23} as shown in Fig. 6 below now enable M_9 to obtain a quorate decision to issue a new membership voucher to M_1.

VI. CONCLUSION

In this paper, we have argued for the value of having a group membership service in ad hoc m-commerce trading forums in order to establish greater trust and more secure interactions among its group members.

Our approach does not rely on a complete knowledge of the current group membership to determine whether a peer is a member of a particular trading forum. Furthermore, it does not demand all group members to participate in group communications frequently and regularly in order for a quorate decision for group membership management to be able to be obtained. However, as the attestation process does not involve any authority higher than a peer and is done independently by each peer based on their partial knowledge of group membership, membership claims acceptable to a sufficient number of peers to qualify may not be found acceptable by every other reasonable peer.

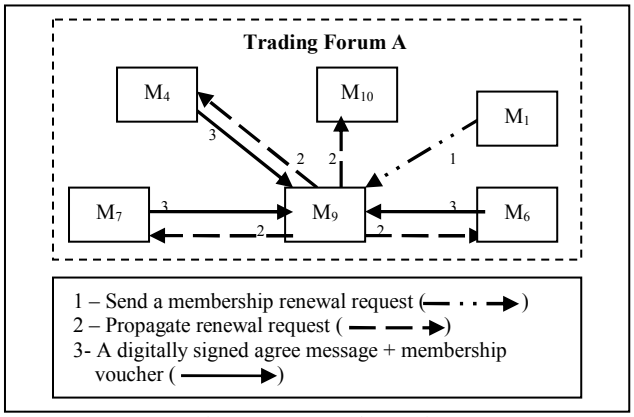

Figure 5. A renewal scenario

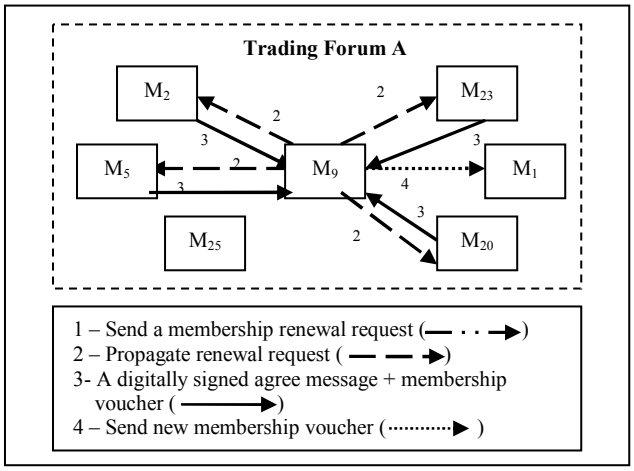

Figure 6. Issuance of a new membership voucher.

With this work, we aim to improve the security of ad hoc m-commerce trading systems by restricting participation to parties regarded as trustworthy by their peers. Our future work will be to implement and validate the proposed mechanisms with some experimental results.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their valuable and helpful comments in improving this paper.

REFERENCES

[1] H. Osman and H. Taylor, "Towards a reference model for m-commerce over ad hoc wireless networks," *Proc. E-Activity and Leading Technologies (E-ALT) Conference*, 2008, pp. 223-232.

[2] K.S. Barber, R. McKay and T-H. Liu, "Group membership services for dynamically organized sensible agent-based systems," *Proc. 12th. International FLAIRS Conference*, AAAI, 1999, pp. 160-165.

[3] A. Ricciardi and K. P. Birman, "Process membership in asynchronous environment," Technical Report TR 93-1328, Department of Computer Science, Cornell University, 1993, pp. 1-42.

[4] G. Roman, Q. Huang and A. Hazemi,"On maintaining group membership data in ad hoc networks," Technical Report WUCS-00-26, Washington University, 2000, pp. 1-11.

[5] S. Maki, T. Aura and M. Hietalahti, "Robust membership management for ad-hoc groups," *Proc. 5th Nordic Workshop on Secure IT Systems)*, 2000.

[6] M. Steiner, G. Tsudik and M. Waidner, "Key agreement in dynamic peer groups," IEEE Transactions on Parallel and Distributed Computing, vol. 11, no. 8, IEEE, 2000, pp. 769-780.

[7] P. Adusumilli, X. Zou and B. Ramamurthy., "DGKD: Distributed group key distribution with authentication capability," *Proc. IEEE Workshop on Information Assurance and Security*, IEEE, 2005, pp. 286-293.

[8] A. Sjoholm, L. Seitz and B. Sadighi, "Secure communication for ad-hoc, federated groups," *Proc. 7th Symposium on Identity and Trust on the Internet*, ACM, 2008, pp. 48-58.

[9] M. K. Sbai, E. Salhi and C. Barakat, "A membership management protocol for peer-to-peer services in MANET," INRIA-00342691, version 2, 2009, pp. 1-9.

[10] P. Pradan and A. Helal, "An efficient algorithm for maintaining consistent group membership in ad hoc networks," *Proc. 23rd International Conference on Distributed Computing Systems*, IEEE Computer Society, 2003, pp. 428-433.

[11] K.-Y. Rhee, Y.-H. Park and G. Tsudik, "A group key management architecture for mobile ad-hoc wireless networks," Journal of Information Science and Engineering, vol. 21, 2005, pp. 415-428.

[12] M. Filali, V. Issarny, P. Mauran, G. Padiou and P. Queinnec, " Maximal group membership in ad hoc network," in Lecture Notes in Computer Science, Springer Berlin, 2006, pp. 51-58.

[13] J. Liu, D. Sacchetti, F. Sailhan and V. Issarny, "Group management for mobile ad hoc networks: design, implementation and experiment," *Proc. 6th. International Conference on Mobile Data Management*, ACM, 2005, pp. 192-199.

[14] D. Bottazi, R. Montanari and G. Rossi, "*A self-organizing group management middleware for mobile ad-hoc networks*," Computer Communications, vol. 31, no. 13, Elsevier, 2008, pp. 3040-3048.

[15] L. Briesemeister and G. Hommel, "Localized group membership service for ad hoc networks," *Proc. International Conference on Parallel Processing Workshops*, IEEE Computer Society, 2002, pp. 94-100.

[16] L. Galluccio, G. Morabito and S. Palazzo, "Spontaneous group management in mobile ad hoc networks," Wireless Networks, vol. 10, no. 4, Kluwer Academic Publishers, 2004, pp. 423-438.