Identity Support in a Security and Trust Service for 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* – Ad hoc m-commerce is an emerging way of conducting online trading wirelessly within dynamic network communities. However, it requires its security and trust issues be properly understood and addressed in order to create sufficient confidence among traders to participate in its transactions. Participants of such trading systems are vulnerable to attacks on identity such as spoofing and whitewashing as well as to fraudulent and unfair trading practices. As security and trust are essential factors in the realization of ad hoc m-commerce, this paper addresses the most common threats and attacks that might have significant effects on the security of such trading systems. In tune with the dynamic nature of ad hoc wireless networks and the social characteristics of ad hoc m-commerce, a scheme for identity support is presented that employs a public key cryptographic mechanism in a fully self-organised manner, where a trading pseudonym and photograph are used as identity credentials in a PGP certificate. The scheme lets participating parties collaborate in a Peer-to-Peer (P2P) way to establish their online identity without any mediation of a Certification Authority (CA). It also enables participating parties to handle the security settings of the trading system as well as share knowledge about the trading behaviour of fellow participants without having to rely on support from a network service provider.**

Keywords – casual local trading, collaborative service, ad hoc community, infrastructure-less service

I. INTRODUCTION

An ad hoc m-commerce trading system is a type of casual local trading facility conducted online and wirelessly outside established computer networks. It enables mobile users with suitable networking capability and appropriate software applications to organise themselves into a trading forum regardless of time or location without relying on any infrastructure support from a network service provider [1]. Members of a trading forum will utilize their own computing resources and also their neighbours to communicate and participate in trading forum's activities such as m-commerce transactions, group membership management, group decision making, attestation processes and so on. However, since a trading forum's activities and communications among its members are carried out over ad hoc wireless networks and as no network service provider can be relied upon to provide security services, this type of trading system is vulnerable to various types of attacks and also subversive behaviour by its participating parties that can undermine its functionality and dependability. Among the attacks and subversive behaviour are identity spoofing, Sybil attacks, man-in-the-middle, unfair evaluations, collusions and misleading trade descriptions.

Public key cryptography provides a variety of techniques for online identification, which can be used to protect trading parties against security attacks aimed at misrepresenting identity. Such identity support can be used as part of a security and trust service to protect the authenticity, integrity, confidentiality and non-repudiation of the information being exchanged throughout the network, as well as to establish a tight binding between a trader's identity and its reputation or membership information. The identity-reputation binding enables traders to assess the behaviour and trustworthiness of each trader as well as to favour trustworthy and reputable parties to trade with while avoiding dubious or untrustworthy ones to reduce transaction risks. The identity-membership information binding helps traders to determine the validity of each member's membership voucher and also each vote sent by participating parties in collaborative decision making processes for group membership management. In ad hoc m-commerce trading systems, a group membership service [2] can be used to keep track of any changes in a trading forum's membership and help determine the current membership status of each member. It consists of mechanisms for new traders to join a trading forum as well as for the existing members to verify other members' membership and also exclude any members that do not adhere to the trading forum's norms. To be recognised as a member of a particular trading forum, a trader must possess a valid membership voucher that has a sufficient number of votes from recognised members of the forum at the time they participated in the vote, digitally signed by a recognised member of the forum at the time it is issued and its validity period must not have expired.

Taking into account the nature of ad hoc wireless networking and the social characteristics of ad hoc m-commerce [1], this paper presents a scheme for identity support for a security and trust service that utilises the self-organizing and infrastructure-less nature of an ad hoc

wireless network. It allows traders in an ad hoc m-commerce trading system to establish their own online identity using Pretty Good Privacy (PGP) technology that uses a trading pseudonym and photograph as identity credentials in PGP certificates and supports a self-revocation mechanism. It also lets the traders collaborate in a P2P manner to handle the attestation process of those identities as well as to control the other security elements of the trading system.

The rest of this paper is structured as follows. Section II discusses a number of possible security threats and attacks to ad hoc m-commerce and also their impact on trading systems. Section III describes the essential elements in security and trust services for such trading systems. Section IV discusses the notion of online identity. Section V gives a brief overview of related work. Section VI presents our approach for identity establishment in ad hoc m-commerce trading systems. Section VII explains how a recipient of a PGP certificate in the proposed approach could verify and check that the party who presents the certificate is actually the owner and identified party in the certificate and also shows how the steps taken can mitigate security attacks related to identity misrepresentation. Finally, section VIII concludes the paper.

II. Possible Threats and Attacks

There are a number of possible threats and attacks that can subvert the security of an ad hoc m-commerce trading system. In this work, we will only focus on addressing the most common ones that have significant impact on the functionality and dependability of such trading systems. We identify those threats and attacks and classify them into three main categories as follows:

A. Identity-related issues

Traders in ad hoc m-commerce trading systems are represented by their online identity, which we refer to via their trading pseudonym. Using pseudonyms to participate in online transactions in such a loose ad hoc community exposes them to security attacks such as identity spoofing, Sybil attacks and also whitewashing.

1) Identity spoofing (masquerade)

Identity spoofing is where an ill intentioned trader tries to pass himself off as someone else. The prime risk is that he may use that spoofed identity to defraud other traders.

2) Sybil Attacks

Sybil attack is where an ill intentioned trader creates multiple trading pseudonyms to cheat collective decision making processes and aggregations of multiple people's judgments to subvert the trading system.

3) Whitewashing

A whitewasher is a trader that leaves a particular trading forum and then re-enters with a new identity to hide his bad reputation or misbehaviour.

B. Information-related issues

As communications and activities related to exchange of information in ad hoc m-commerce trading systems are conducted solely over an insecure ad hoc wireless network and may involve intermediary peers, participating parties of such trading systems are also vulnerable to man-in-the-middle attacks. A man-in-the-middle attack is where an ill intentioned trader intercepts communications between two parties and then tampers with or omits messages being transferred without the knowledge of either the original sender or the recipient.

C. Misbehaviour-related issues

With dynamic participations in an ad hoc m-commerce trading forum [2], it is to be expected that traders will often engage in a transaction with parties that they do not have any prior experience of or have never met before. This will make them susceptible to subversive behaviour by their trading counterparties, such as been given misleading trade descriptions or unfair deal evaluations or being subject to repudiation misbehaviour and collusions.

1) Trade Misdescriptions

An ill-intentioned trader may cheat other members of a trading forum by offering fake items as real or by trading items that are not as described in the offer.

2) Unfair Deal Evaluations

In ad hoc m-commerce trading systems, traders are expected to evaluate each other after the completion of the each transaction by generating a deal evaluation. This deal evaluation can be used to assess each trader's reputation and will consist of at least the following information.

a) The evaluator's trading pseudonym.

b) Transaction contract which is digitally signed by both parties and has a timestamp as a proof of a transaction.

c) Evaluation result that records the amount of satisfaction the evaluator receives from his transaction with the owner.

d) Digital signature of the evaluator to protect the integrity of the deal evaluation as well as the information within.

If a transaction concludes positively, traders are expected to express their satisfaction about the transaction in the deal evaluation, digitally sign it and then send it to their trading counterpart. Otherwise, they can share their bad evaluation of their trading counterpart with other traders in the trading forum to make them aware of that party's negative behavior. However, an ill-intentioned trader may manipulate the reputation of other traders by giving unfair evaluations of transactions. There are at least two types of unfair evaluations; overstating and slandering. Overstating is where a trader gives unfair positive evaluations to increase the reputation of a particular party while slandering is where a trader attacks the reputation of other traders by giving unfair negative evaluations to lower the reputation of those parties.

3) Repudiation Misbehaviour

Repudiation misbehaviour occurs when a trader performs a particular action and then denies having performed it. There are at least two significant types of repudiation misbehaviour; data repudiation and contract repudiation. Data repudiation occurs when a trader sends a particular message or document and then denies having sent that message or document. Contract repudiation occurs in a situation where one party initiates a transaction or has agreed on a transaction contract and then denies having initiated the transaction or having agreed on the contract.

4) Collusions

Collusion is where multiple ill-intentioned traders or an ill-intentioned trader with multiple identities conspire to influence their own reputation or other traders' reputation, group decision making processes, attestation processes and so on.

The significant impact that the above threats and attacks have on the security of the trading systems is that they can undermine the functionality and reliability of its reputation service, group membership management [2], attestation processes as well as the transaction activities. For example,

a) A trader may masquerade as a reputable trader by using that trader's identity to induce other traders to transact with him and then defraud them.

b) A trader may create multiple identities to provide bogus support for certificates or membership vouchers.

c) Multiple traders may collude to control collaborative decision making for group membership management.

d) Multiple traders may conspire to give unfair negative evaluations to an honest trader in order to damage that trader's reputation.

e) A trader may escape his bad reputation recorded in previous deal evaluations by leaving the trading forum and then re-entering with a new identity.

f) An intermediary peer may discard or alter a vote that is being transmitted via his node without being detected by the two end parties.

g) A trader may undertake a transaction contract and then deny having made that contract.

III. Security And Trust Service

Thus, to create an environment that is secure and trusted to some sufficient degree for traders to trade within ad hoc m-commerce trading systems, the following elements are essential for its security and trust service.

A. Message authenticity, integrity, confidentiality and non-repudiation

Support for message authenticity, integrity and also non-repudiation is important to give assurance to participating parties that messages or documents being exchanged among them actually originated from the specified sender and were not altered in transit. Also, the receiving peer can be assured that the sender cannot credibly deny having sent the messages or documents. Confidentiality will ensure that messages or documents sent across the network are unreadable by any third parties other than the authorized recipients, such as eavesdroppers or peers that act as intermediaries. Having these elements in the security and trust service will protect traders from man-in-the-middle attacks and repudiation misbehaviour.

B. Trust

The development of a trust relationship among participating parties of any kind of ad hoc m-commerce trading system is vital to mitigate uncertainty and risks involved in the transactions. Parkhe in [3], describes uncertainty in online transactions as uncertainty about unknown future transactions and also uncertainty about potential trading partners' behaviour in fulfilling their transaction agreements. These uncertainties create a perception of significant risk that might discourage traders from engaging in such transactions. A transaction is potentially risky if engaging in it exposes a trader to the chance of significant loss. Loss can be incurred in various ways. For example, not getting what is being traded for is a significant loss. Parting with money and getting goods in exchange that are found to be significantly inferior to what was agreed is also a significant loss. Losing scarce opportunities to trade with others on good terms because one has agreed to trade with someone who then withdraws from the deal or forces inferior terms for the deal on the trader is another way of incurring loss. Loss of reputation is another example of significant loss. Engaging in a transaction with an ill-intentioned trader exposes an honest trader to the possibility of harm to his reputation as the ill-intentioned trader may provide unfair negative evaluations or issue a false complaint that may negatively affect that honest trader's standing.

A trust relationship that is established between two traders will make them believe that their trading counterpart is a sufficiently reliable and honest party to trade with and the likelihood of downside losses is low enough for them to expose themselves to. This will enable them to view the above mentioned risks as acceptable. Thus, by having support for trust in the security and trust service, security issues related to trader's subversive behaviour such as giving misleading trade descriptions can be mitigated.

Greater trust and more secure interactions among traders can be established through a group membership service and sanctions mechanism [2]. A group membership service helps to improve the security of the trading system by restricting participation to parties considered as trustworthy by other peers while a sanctions mechanism helps mitigate security issues such as unfair evaluations and collusions. The sanctions mechanism enables members of the trading system to exclude any of its members who conduct themselves inappropriately, if there is complaint about their

misbehaviour from other members and also an exclusion proposal.

C. Attestation

Attestation is significant as it provides a means for traders to vouch for other parties' credentials such as their digital certificates, membership status, reputation reports and also trading histories. It also helps to mitigate transaction risks, especially in situations that involve dealing with unfamiliar trading counterparties.

D. Identity Support

Among the other elements, identity support is probably the most important element in a security and trust service for an ad hoc m-commerce trading system. Robust identification support will not only protect traders from security attacks targeting at identity disguise, but it also enables the other elements of a security and trust service to function properly and effectively. It provides a kind of security assurance for participating parties to communicate, collaborate, carry out transactions, exchange information, manage group membership and also establish trust relationships among themselves.

IV. The Notion Of Online Identity

In online trading, traders are represented by online identities. An online identity refers to a social identity that is established by users as a means to represent themselves in online communities. The main choice here seems to be between using their real identities such as their legal name, date of birth and home address or a trading pseudonym to represent themselves online.

The use of a trading pseudonym would enable traders to participate in online trading incognito. It would also allow traders to keep their trading behaviour such as purchasing or gambling behaviour discrete and thus protect their privacy. Furthermore, it would enable traders to project a persona that was distinct from their own. For example, a pseudonym of Honest Eddy or the Professor could signify a style of approach to trading that reinforces a reputation they wish to maintain. The real identity of a trader in terms of their legal name, date of birth and home address is not necessarily a relevant issue in online trading. The reputation of a trading pseudonym can be compromised just as easily as the reputation associated with a real identity. So the value of maintaining that reputation can act as a strong disincentive to abusing a trading pseudonym. By linking together reputation to a trader's pseudonym, the trustworthiness as well as future behaviour of that trader can be evaluated and predicted as long as a persistent identity is used. Pseudonyms make things harder where parties seek legal redress against criminal trading practices or against torts (contract violations) in civil law. However, in casual local trading such recourses to law are rare and anyway the problem of converting a trading pseudonym to the real identity behind it is not insuperable.

In ad hoc m-commerce trading systems, using real identities would create a problem of verification as no CA can be relied upon to have checked a trader's real identity credentials such as his identity card or driving licence or passport to verify his identity. Attestors of such identities would have to assure themselves that a trader was entitled to call himself by his purported legal name, was actually born on the stipulated date and genuinely resided at the stated address which is hard to be sure of. However, in practice casual trading attestors want to attest an identity established by a recognised appearance and a recognised form of address for trading purposes. What the subjects are really called or when they are born or where they really live is normally beside the point. Also, using real identities can make it harder for traders to maintain secrecy about their engaging in particular transactions. Lack of secrecy can threaten a trader's privacy, put them at risk of harm from hostile competitors or even compromise the profitability of deals that they undertake. However, allowing pseudonyms raises the question of whether traders can change their presented identity or create multiple identities in order to hide their bad behaviour or reputations. Traders might also try to hide their relation to a particular action and thus have a chance of avoiding being held accountable for that action. To prevent these issues in ad hoc m-commerce trading systems requires robust identification of traders. We propose doing this with digital certificates in a manner to be described in Section VI.

V. Related Work

A significant amount of research has been done in the area of public key management in ad hoc wireless networks and several solutions have been proposed in the literature [4-17]. This section will discuss briefly some of it which is relevant to our work. Abdul Rahman in [10] has proposed using the PGP Trust Model that allows users to generate their own asymmetric key pairs as well as to function as independent CAs. Thus, any user in the network can sign and verify any other user's public key. These signatures progressively form a set of interconnected links of individual public keys or "Web of Trust" [8, 9]. The main interest in this model is that it does not require a communal certification authority to vouch for a user's public key. However, Rahman's scheme requires a central key server to maintain a database of public keys which makes his approach unsuitable for ad hoc m-commerce trading systems as the responsibility for hosting the key server will be problematic in such a loose trading community with frequent network disconnections and irregular participation. It will be difficult or impossible to resolve who would be responsible for providing and paying for the server and also whether all users would trust them to do that. Furthermore, uninterrupted connectivity with such a key server could not be guaranteed in such a network.

Capkun et al. in [11] have proposed a fully self-organized approach to public key management that does not rely on any trusted authority or centralized infrastructure. It allows users to generate their own public key pairs, issue

digital certificates to other users and also perform authentication with each other by merging their local certificate repositories and then evaluate the authenticity of the public key based on the certificates available in the merged repository. Interesting aspects of this approach are that it enables users to control the security settings of the system and also to perform key authentication based on the available information in each user's local repository. In addition to that, it does not require participation by all users during the authentication process. This approach seems to be suitable for our work due to its self-organized characteristic. However, its certificate renewal mechanism requires the same issuer to issue a new updated version of certificate to the same user and would not be appropriate in our work as regular participation by trading parties could not be guaranteed in such trading systems. Traders with expired certificates would be at serious risk of having to wait for a long time in order to get in contact with their same certificate issuer. They might not even be able to get in contact with those issuers ever if those issuers no longer participate in the trading system or have been excluded from the trading forum.

Another fully self-organized approach has been described by Rachedi and Benslimane in [12]. In their approach, they propose a distributed clustering algorithm to select a cluster head in each cluster, which is based on a trust value and mobility metric. The cluster head then becomes the CA in its cluster. This approach does not seem to be workable either in ad hoc m-commerce trading systems as participation by the cluster head in the trading forum cannot be guaranteed all the time, and thus will make the attestation process unreliable. Furthermore, the role of a cluster head does not seem to be appropriate in a community of traders who regard each other as equals. Also, it cannot be expected that any prospective cluster head will be sufficiently trusted by all other traders in that cluster. While some parties will be trusted more than others by their fellow traders, many trading communities lack any prospect of achieving a consensus about which parties among them are worthy of enhanced trust.

VI. Our Approach

The motivation for employing our approach comes from the self-organizing and infrastructure-less nature of ad hoc wireless networks and also the necessity to allow collaboration among participating parties of an ad hoc m-commerce trading system to control its security settings. In this work, support for identity establishment will include generating public and private key pairs, generating and signing PGP certificates, verifying the certificates as well as revoking compromised certificates. The verification process will be done in a P2P manner without the intervention of a CA. All participating parties will play a similar role. We assume that:

a) Each trader will maintain their own local certificate repository that contains their own certificate and other parties' certificates that they have attested or been in contact with before.

b) Each trader will create their own trading pseudonym. To avoid more than one trader using the same pseudonym, each trader is expected to check for this possibility against all trading pseudonyms that are used by certificates in their local certificate repository or that they have stored a record of having heard of before attesting other parties' certificates.

c) A trader will verify other traders' certificates based on his knowledge and also recommendations from his other peers that he regards as credible as detailed in Section VII.

A. The creation of public/private key pairs

Using PGP technology [8, 9], each trader will create their own private-public key pairs locally.

B. The generation of digital certificates

Traders will also generate their own self-signed digital certificates locally. The format of the certificates will be in the form of PGP certificates. Each certificate will contain at least the following information:-

1) The certificate holder's public key.

2) The certificate holder's identity credentials.

We propose using the holder's trading pseudonym and a photograph as their identity credentials. A photograph is used as part of a trader's identity credentials because it is more convenient and realistic to use than other information such as home address or email address or date of birth when it comes to a verification process. To do the verification, attestors can check the photograph against the appearance of party who asserts the enclosing certificate identifies them. One way to do the checking is by having a physical encounter which should be easy as traders trading via ad hoc networking are likely to be in close proximity with each other. In addition to allowing more convenient and realistic verification, the use of a photograph can be one of the most appropriate solutions to defend against Sybil attacks and whitewashing as traders cannot easily change their physical appearance and it will be detectable when multiple identities have similar photographic appearances.

3) The digital signature of the certificate owner.

4) The certificate's validity period.

Each certificate will be issued with a standard limited validity period. Traders will have to generate their new self-signed certificate before the existing one expires and then send the newly generated self-signed certificate together with their current certificate to any members of the trading forum that they believe to be trustworthy for certificate verification. Certificates need to be time limited to some degree such as 5 years because aging changes physical appearance creating a mismatch with a photo. Short validity periods for certificates are probably undesirable to avoid the overheads of their renewal too frequently.

5) The digital signature(s) of the certificate's attestor(s) and their certificate identifiers.

Multiple signatures on a single certificate give more assurance to the relying parties that the photograph and trading pseudonym in the certificate accurately identify a party with knowledge of the corresponding private key.

Traders will store their own certificate and the certificates of other parties that they have been in contact with previously in their local certificate repository.

C. The verification of digital certificates

Since there is no inherent association between a public key and the identity credentials listed in the self-signed digital certificates, the validity of such certificates need to be attested by other parties to avoid an-ill intentioned trader from masquerading as others. In ad hoc m-commerce trading systems, as participating parties are peers who consider each other as equals, any peer can vouch for another peer's digital certificate. However, the validity of such a certificate will only be accepted if the relying party recognises a party who has vouched for the certificate as a trusted party. This process is based on the concept of a web-of-trust [8-10]. For example, if peer A trusts peer B sufficiently as an attestor, it is expected that peer A will accept the validity of peer C's digital certificate that is vouched by peer B. Anyone who trusts the attestor as an attestor, will consider any certificates signed by the attestor to be valid to the extent of that trust. To lessen the risk that any one certificate signatory is unknown or untrusted as an attestor, multiple signatories will usually be required.

D. Certificate Revocation

Any traders that believe their private key has been compromised can revoke their own certificate by performing the following steps:-

1) First, generate a new private-public key pair.

2) Second, generate a new self-signed certificate that binds their identity credentials with the newly created public key. Traders are expected to use the same trading pseudonym for their identity credentials in order to maintain a persistent identity, so that their reputation can be retained.

3) Third, send the newly-generated self-signed certificate to any members of the trading forum that they believe to be credible to attest the validity of the certificate. Also they need to send their old certificate with it in order to use the same trading pseudonym.

4) Finally, inform other members of the forum about the revocation of their certificate by multicasting a revocation message signed by the new and old private keys together with the new and old certificates. The receiving peers will update their local certificate repository by marking the old certificate as "compromised" and adding the new certificate to the list, if the signatures on the revocation message check out and their photos correspond. Otherwise the message and new certificate will be ignored.

If any traders discover evidence that a particular trader's certificate has been compromised, they can inform its holder as it is the responsibility of that trader to revoke its own certificate by performing the above steps.

VII. Discussion

In this section, we explain how a recipient of a PGP certificate in our approach would check and verify the identity stated in it to assure that it really belongs to the party that presents the certificate and show how the steps taken can make it difficult for an ill-intentioned trader to masquerade as others or create multiple identities or be a whitewasher. To do the checking and verifications, a trader performs the following steps upon receiving a digital certificate from other traders that he has never dealt with before. Some of the steps may require further checks depending on the outcome of the check or how careful the recipient is in checking the credibility of the other party that he is dealing with. Some may only be important if the currently proposed transaction has significant downside risks and the receiving parties want to be assured that the presenting party has a good trading history.

1) Check the trading pseudonym in the certificate against their store of certificates to see if a different certificate uses the same trading pseudonym. This step helps the recipient to discover attempts by an attacker to spoof the identity in that certificate. In this situation, the recipient should reject the presented identity as bogus if there is another certificate in his local certificate repository that use the same trading pseudonym yet has a photo of an obviously different person.

2) Check whether the presenter is able to sign a message that is verified by the certificate's public key. This will ensure that the presenter knows the private key for that certificate's public key. However, this check alone is not enough to determine that the presenter is actually the real owner of the certificate as he could have compromised the real private key and then be masquerading as that certificate's identity. Although the recipients of such certificates can do a photo check against the appearance of the presenting party when they come into close proximity with each other (step 4), they might not be able to detect such an attempt as the presenter could have generated a new certificate containing the spoofed party's public key and trading pseudonym but his own photo. He could also have generated a new certificate with a new public key, his own photograph and the trading pseudonym of the party whose identity he wants to hijack.

3) Check the self signature against the certificate's public key to ensure that the presenting party has not altered the contents of the certificate like the certificate's validity period or its owner's photograph. This step will protect against man-in-the-middle attacks.

4) Check the photo against the appearance of the subject when they are in a close proximity with each other. This

step enables the recipient to compare the real physical appearance of the presenting party with the photo in the presented certificate in the case that the recipient wants to be assured that there is no attempt by the subject to spoof another party's identity after discovering that party's private key.

5) Check the photo against their store of certificates to see if that appearance is used with a different identity. This step could enable the recipient to detect an attempt by the presenting party to create multiple identities in order to manipulate the reputation system or collaborative decision making in group membership management or attestation processes. It also can make it possible for the recipients to unmask whitewashing for example, an attempt by a party that has a bad trading history or has been excluded from a trading forum's membership to re-enter with a new identity.

6) Check that a certificate with that public key is not recorded as 'compromised' in his local certificate repository. This will prevent the attacker from further abusing a spoofed identity. It could also be used as an evidence to exclude the presenter from a trading forum's membership for conducting himself inappropriately.

7) Check whether the certificates of any trusted third parties that have signed the presented certificate are available in his local certificate repository. They can provide reassurance that the presenting party with the given appearance is entitled to use the trading pseudonym. Any attempt by those third parties to attest a false identity of the presenting party could expose them to the risk of being excluded from a trading forum's membership. This provides a modicum of accountability for subversive behaviour.

8) Check that the photo appearance is not very similar to that of anyone that there have been broadcast warnings about, for example for spoofing other party's identities or against whom an exclusion proposal has been issued and so on. This will give some kind of assurance to the recipient that the certificate is not of a known malefactor. It also throws suspicion on the good faith of signers of the certificate.

9) Check the validity date on the certificate has not expired. An expired certificate doesn't disapprove the identity of its presenter but it does raise doubts about the usefulness of the photo and about whether the presenter has had difficulties finding trustable third parties to sign a current certificate for that party.

To mitigate security issues related to misbehaviour of a trader, a distributed reputation system will be used as a means to facilitate trust development among participating parties as it provides a collaborative method to assess the behaviour and the trustworthiness of each trader. It also makes it possible for the participating parties to identify and sanction those who misbehave or violate the ethical norms of the community. It increases the likelihood of reputable and trustworthy traders to be favoured as trading partners and thus helps mitigate uncertainty and risks involved in the transaction such as misleading trade descriptions by trading counterparties. A trader's public key and a transaction contract that is digitally signed by both parties involved in the transactions, which are included in the deal evaluations after the transaction will establish a tight binding between a trading party's identity and its reputation.

Unfair evaluations and collusions are probably the most challenging issues in an ad hoc m-commerce reputation service as well as in any reputation system as it is difficult to control the sincerity of traders in providing their deal evaluations. Some proposed solutions [18-20] make the assumption that a reputable trader will also provide deal evaluations honestly. However, this is not always true as a trader may carry out each transaction honestly but not be fair in providing deal evaluations. They may be sceptical about other parties' good faith. There are also solutions [21-22] that provide monetary and other incentives to encourage participating parties to provide honest evaluations. However, such incentives are not applicable in this work as they require a central authority to administer the evaluation payments as well as providing little guarantee that the participating parties will provide truthful evaluations. In this work, unfair evaluations and also collusions are discouraged by deploying a sanctions mechanism. Traders who make inappropriate negative or positive evaluations or conspire with other parties to influence their own reputation or others' reputation are open to the risk of being excluded from a trading forum's membership if other members of the forum receive complaints about their misbehaviour and also an exclusion proposal. To ensure that a trader is not excluded from a trading forum unfairly, the decision to exclude any party will be based on quorate decision making involving other members of the forum [2], where forum members with views on the proposal would be given an opportunity to participate in the exclusion vote. Trading forums will be able to tune the stringency of the votes required for exclusion to balance the risks of unfair decisions and collusions against unwanted exclusions. A trader's digital signature on each vote and also exclusion proposal will provide assurance to the receiving parties that the vote or exclusion proposal was sent by a particular sender and was not tampered with during transmission. That sender also cannot get away with denying having sent such a vote or exclusion proposal. This will avoid the ill-intentioned trader from sending false exclusion proposals or colluding with each other to manipulate the votes as their digital signatures will prove that those messages were originated by them, and thus will be the evidence for other members to exclude them from a trading forum's membership for such misbehaviour. Also, it will be difficult for a trader to masquerade as others to send such a vote or exclusion proposal without being detected by others as discussed in the steps above.

VIII. CONCLUSION

With this work, we introduce a novel form of support for ad hoc m-commerce that aims to create a sufficient degree

of confidence among traders to participate in such a casual local wireless trading, as well as to serve as a basis for establishing a m-commerce domain in a totally self-organizing and P2P manner. In the design of a security and trust service for such trading systems, we have identified and discussed three main categories of common threats and attacks that have significant affects on its security. We believe that by addressing these three main categories of threats and attacks, an environment that is sufficiently secure and trusted can be created for traders to communicate, collaborate and carry out transactions. We also believe that by providing robust identification support, such security threats and attacks can be prevented or at least mitigated.

In addition to that, we have discussed the notion of online identity in the context of online trading. We propose a mechanism that allows participating parties of an ad hoc m-commerce trading system to establish their online identity in a fully self-organizing manner using a trading pseudonym and a photograph as their identity credentials in a PGP certificate. It also allows collaboration among those parties to control the attestation process of such PGP certificates without relying on any trusted certification authority. The use of a trading pseudonym and a photograph as a trader's identity credentials and a self-revocation mechanism in our approach are offered as an appropriate way to deal with identity establishment in such a dynamic ad hoc trading community. We discussed the steps that can be performed by a recipient of such a PGP certificate in our approach to resist security attacks against online identity. We intend that this work together with our proposed group membership service [2] and a reputation system under design will be able to support security for an ad hoc m-commerce trading system to a sufficient degree for trade to be viable using it.

However, real life experiences in conducting such online trading in this way are still required to evaluate the effectiveness of the proposed approach as well as to discover other possible security attacks. Our future work will attempt to validate our proposed security and trust service with some experimental results using real life scenarios and security expert reviews.

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] H. Osman and H. Taylor, "Managing group membership in ad hoc m-commerce trading systems", *Proc. 10th. Annual International Conference on New Technologies of Distributed Systems*, 2010, IEEE, pp. 173-180.

[3] A. Parkhe, "*Understanding trust in international alliances".* Journal of World Business, vol. 33, no. 3, Elsevier , 1998, pp. 219-240.

[4] P. Michiandi and R. Molva, "*Ad hoc networks security*," ST Journal of System Research, vol. 4, no. 1, 2003, pp. 756-775.

[5] Z. Liu, et al. "A dynamic trust model for mobile ad hoc networks," *Proc. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems*, 2004, IEEE, pp. 80-85.

[6] L. Butyan, and J.-P. Hubaux, "Security and cooperation in wireless networks: Thwarting malicious and selfish behaviour in the age of ubiquitous computing," 2008, Cambridge University Press. p. 74-77.

[7] J. Sen, P.R. Chowdhury, and S. Indranil, "A distributed trust establishment scheme for mobile ad hoc networks," *Proc. International Conference on Computing: Theory and Applications*, 2007. p. 51-58.

[8] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume I* 1993. [cited 20/10/09]; Available from: http://www.geocities.com/Athens/1802/pgpdoc1.html

[9] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume II*. 1993. [cited 20/10/09]; Available from: http://www.geocities.com/Athens/1802/pgpdoc2.html.

[10] A. A. Rahman, "*The PGP trust model*," 1996, Department of Computer Science, University College London: London. pp. 1-6. [cited 01/07/09] Available from : http://netresearch.ics.uci.edu/Previous_research_projects/agentos/related/security/abdul-rahman-pgp-trust.pdf

[11] S. Capkun, L. Buttyan and J. Hubaux "*Self-organized public key management for mobile ad hoc networks*," IEEE Trans Mobile Computing, vol. 2, no. 1, 2003, IEEE, pp.52-64.

[12] A. Rachedi and A. Benslimane, "Trust and mobility-based clustering algorithm for secure mobile ad hoc networks," *Proc. International Conference on Systems and Networks Communication*, IEEE, 2006, pp. 72-77.

[13] E. C. H. Ngai and M. R. Lyu, "Trust and clustering-based authentication services in mobile ad hoc networks," *Proc. 24th. International Conference on Distributed Computing Systems Workshop*, IEEE, 2004, pp. 582-587.

[14] D. S. Thenmozhi and R. Murugan, "Security association in mobile ad hoc networks through self-organized public key certification," *Proc. 4th. International Conference on Applied Mathematics and Computer Science*, ACM, 2005.

[15] L. Cai, J. Pan, X. S. Shen and J. W. Mark, "*Promoting identity-based key management in wireless ad hoc networks*," Wireless Network Security, vol. 4, no. 2, 2007, Springer, pp. 83-102.

[16] B. Wu, et al. "*Secure and efficient key management in mobile ad hoc networks*," Journal of Network and Computer Applications, vol. 30, no. 3, 2007, Academic Press Ltd , pp. 937-954.

[17] M. Omar, Y. Challal and A. Bouabdallah, "*Reliable and fully distributed trust model for mobile ad hoc networks*," Computer and Security, vol. 28, no. 3-4, 2009, Elsevier , pp. 199-214.

[18] A.B. Can and B. Bhargava," SORT: A self-organizing trust model for peer-to-peer systems*"*, 2006.

[19] L. Xiong and L. Liu, "A reputation-based trust model for peer-to-peer e-commerce communities," IEEE International Conference on E-Commerce, 2003, *IEEE* , pp. 275-284.

[20] C. Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," *Proc. 2nd. ACM Conference on Electronic Commerce*, ACM, 2002, pp. 150-157.

[21] N. Miller, P. Resnick and R. Zeckhauser, "Eliciting honest feedback in electronic markets," [cited 15/01/2009] 2002; http://ksgnotes1.harvard.edu/Research/wpaper.nsf/46ad8749e613af608525693c0014d6cc/d997a59b1cb907cb85256c39004c241c/$FILE/elicit.pdf, pp. 1-31.

[22] R. Jurca and B. Faltings, "An incentive compatible reputation mechanism," *IEEE International Conference on E-Commerce*, 2003, IEEE, pp.285-292.