Identity support in a security and trust service for ad hoc m-commerce trading systems

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, participants in such systems are vulnerable to attacks on identity establishment such as spoofing and whitewashing as part of fraudulent and unfair trading practices. This paper presents a scheme for identity support using PGP certificates in a fully self-organised manner, where a trading pseudonym and photograph are used as identity credentials. It lets participating parties collaborate in a Peer-to-Peer (P2P) way to establish their online identity in a manner that is resistant to such attacks without any mediation of a Certification Authority (CA). It also lets participating parties handle the security settings of the trading system as well as share knowledge about fellow participants' trading behaviour without relying on support from a network service provider.**

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

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 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 available computing resources to communicate and participate in activities such as m-commerce transactions, membership management, attestation processes and so on. However, since such activities 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 that undermine its functionality and dependability. These include identity spoofing, Sybil attacks, man-in-the-middle attacks, unfair evaluations, collusions and misleading trade descriptions.

Public key cryptography provides a variety of techniques for online identification, which can be used to protect traders against attempts to misrepresent 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 information being exchanged, as well as to establish a tight binding between a trader's identity and its reputation and membership information. The identity-reputation binding enables traders to assess the trustworthiness of other traders. The identity-membership information binding helps traders to determine the validity of each member's membership voucher and also each vote made by participating parties in collaborative decision making processes for membership management. In ad hoc m-commerce trading systems, a membership service could keep track of a trading forum's membership and help determine the current membership status of each participant. It would consist of mechanisms for traders to join, to verify other parties' membership and to exclude those that do not adhere to the trading forum's norms. Our scheme proposes that to be recognised as a member of a trading forum, a trader must possess a valid membership voucher that has a sufficient number of votes from recognised members of the forum, is digitally signed by a recognised member that issues it and its validity period must not have expired [2].

However, ad hoc m-commerce trading systems lack infrastructure services to support public key cryptographic mechanisms that rely on a trusted CA. They also cannot support self-organised substitutes that require one or more parties to be the certification authority for other peers as participation by those parties on a regular basis cannot be guaranteed in such a dynamic trading community. Identity establishment in ad hoc m-commerce trading systems requires a scheme that is peer to peer, independent of a pre-established network infrastructure and able to support infrequent communications among traders. This paper presents such a scheme for identity support for a security and trust service. It lets traders in an ad hoc m-commerce trading system 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 other security elements of the trading system.

The rest of this paper is structured as follows. Section II discusses possible security threats and attacks on ad hoc m-commerce and their impact on trading systems. Section III describes the essential elements in security and trust services for such systems. Section IV discusses the notion of online identity. Section V critically assesses related work. Section VI presents our approach for identity establishment

978-0-7695-4338-3/11 $26.00 © 2011 IEEE
DOI 10.1109/WAINA.2011.85

in ad hoc m-commerce trading systems. Section VII concludes the paper.

II. Possible Threats and Attacks

There are several possible threats and attacks that can subvert the security of an ad hoc m-commerce trading system. We only focus on addressing the most common ones that significantly impact the functionality and dependability of such systems. We identify those threats and attacks and classify them into three categories:

A. Identity-related issues

Traders in ad hoc m-commerce trading systems are represented by their online identity, which we propose to handle with trading pseudonyms. Using pseudonyms to participate in online transactions in such a loose ad hoc community exposes them to the following security attacks.

1) Identity spoofing (masquerade)

Identity spoofing is where a party tries to pass himself off as someone else. The prime risk is that he may use that spoofed identity to defraud others.

2) Sybil Attacks

Sybil attack is where a party creates multiple identities to cheat collective decision making processes to subvert the trading system.

3) Whitewashing

A whitewasher is a party who leaves a particular forum and then re-enters with a new identity to hide his bad reputation.

B. Information-related issues

As exchanges of information in ad hoc m-commerce trading systems are conducted solely over insecure ad hoc wireless networks and may involve intermediaries, participants in such trading systems are vulnerable to man-in-the-middle attacks. Such an attack occurs when a party intercepts communications between two other parties and then tampers with or omits messages being transferred without the knowledge of either sender or recipient.

C. Misbehaviour-related issues

In ad hoc m-commerce trading systems, it is to be expected that traders will often engage in transactions with unfamiliar parties. This will make them susceptible to subversive behaviour by their trading counterparties such as:

1) Trade Misdescriptions

A party may cheat other traders 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 could be required to evaluate each other after the completion of each transaction by means of deal evaluations. They could be used to assess each trader's reputation and could 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 the trade.

d) The evaluator's digital signature.

If a transaction concludes positively, traders could be required to express their satisfaction in the deal evaluation, digitally sign it and then send it to their trading counterpart. Otherwise, they could share their bad evaluation with other traders in the trading forum. However, an ill-intentioned trader might manipulate the reputation of other traders by giving unfair deal evaluations. There are at least two types of unfair evaluations; overstatements and slanders. Overstatements give inaccurate positive evaluations to increase the reputation of a particular party while slanders attack the reputation of trading counterparties by giving inaccurate negative evaluations to lower their reputation.

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 such misbehaviour; data and contract repudiations. Data repudiation occurs when a trader sends a message or document and then denies having sent it. Contract repudiation occurs when one party initiates a transaction or agrees on a transaction contract and then denies having initiated the transaction or having made the contract.

4) Collusions

Collusion is where multiple parties or a party with multiple identities conspire to influence their own or other traders' reputation, group decision making processes, attestation processes and so on.

The significant impact that these attacks have on the security of the trading systems is that they can undermine the reliability of the following:

a) The reputation service, e.g. a trader may conspire with associates to influence his own or other traders' reputations by providing unfair deal evaluations, which lead other traders into making incorrect trust decisions that result in unsatisfactory transactions.

b) Group membership management, e.g. multiple traders may collude to subvert collaborative decision making for group membership management or an intermediary may discard or alter a vote that is sent via his node without being detected by the end parties

c) Attestation processes, e.g. a trader may create multiple identities to provide bogus support for certificates.

d) Transaction activities, e.g. a trader may undertake a contract and then deny having made it.

III. Security And Trust Service

To create a sufficiently secure and trusted environment for traders to trade within ad hoc m-commerce trading systems, its security and trust service needs support for:

A. Identity

Identity support is probably the most crucial element in a security and trust service for an ad hoc m-commerce trading system. Robust means of identification will not only

protect traders from attacks aimed at identity disguise, but also lets other elements of a security and trust service function properly and effectively. It provides a kind of security assurance for traders to communicate, collaborate, carry out transactions, manage membership and establish trust relationships with known other parties.

B. *Message authenticity, integrity, confidentiality and non-repudiation*

Support for message authenticity, integrity and non-repudiation is important to give assurance to participating parties that messages or documents being exchanged among them originated with their specified sender and were not altered in transit. Also, the recipients can be assured that the sender cannot credibly deny having sent them. Confidentiality will ensure that they are unreadable by eavesdroppers or intermediaries. Having these elements in the security and trust service will protect traders from man-in-the-middle attacks and repudiation misbehaviour.

C. *Trust*

The development of trust relationships among traders is vital to mitigate uncertainty and risks involved in the transactions. Parkhe in [4], describes uncertainty in online transactions as uncertainty about future transactions and about potential trading partners' behaviour in fulfilling their transaction agreements. These uncertainties create a perception of significant risk that might discourage traders from trading. A trust relationship established between two traders lets them believe that their counterpart is a sufficiently reliable and honest party to trade with and that the downside risks are low enough for them to expose themselves to. Thus, by having support for trust in the security and trust service, security issues related to potential misbehaviour can be mitigated.

D. *Attestation*

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

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 to a certain degree private. Furthermore, it would enable traders to project a distinctive trading persona 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 normally 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 contract violations. 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 needed in legal cases 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 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 for other traders 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 were born or where they really live is 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 issue of whether it allows traders to create multiple identities or change their presented identity too easily. Traders might also try to hide their relation to a particular action like an attestation or vote and thus avoid 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 [5-18]. This section will discuss briefly those which are relevant to our work. Rahman [11] has proposed using the PGP Trust Model to let users 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" [9, 10]. The main interest in this approach 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. 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. [12] have proposed a fully self-organized approach to public key management that does not rely on any trusted authority or centralized infrastructure. It lets users generate their own public key pairs, issue digital certificates to others and authenticate each other by merging their local certificate repositories and then evaluate the authenticity of a public key based on the certificates available in the merged repository. Interesting aspects of this approach are that it enables users to distribute control of the security settings of the system and also to perform key authentication based on the available information in each user's local repository. It also does not require participation by all users during the authentication process. This approach seems to be suitable for our work due to its self-organised characteristic. However, its certificate renewal mechanism requires the same issuer to update a user's certificate and would not be appropriate in our work as regular participation by trading parties cannot be guaranteed. Traders with expired certificates would be at serious risk of having to wait for a long time to get in contact with their certificate issuer or never succeed if the issuer is no longer active or has been excluded from the trading forum.

Another fully self-organised approach has been described by Rachedi and Benslimane [13]. 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. The status of a CA node will change if other nodes do not receive any beacon from its node for a pre-defined period of time and a new CA will be elected. This approach does not seem to be workable either in ad hoc m-commerce trading systems as frequent changes in the CA role will make the attestation process unreliable. Furthermore, the role of a cluster head does not seem to be appropriate in a community of 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 our approach comes from acknowledging the self-organizing and infrastructure-less nature of ad hoc wireless networks and allowing participants in ad hoc m-commerce trading systems to control their security settings. Support for identity establishment will include generating public and private key pairs, generating, signing and verifying PGP certificates as well as revoking compromised certificates. The verification process will be done in a P2P manner without the intervention of a CA. All participants will play a similar role. We assume that:

a) Each trader maintains their own local certificate repository that contains their and other traders' certificates that they have attested or acquired.

b) Each trader creates their own trading pseudonym. To minimise the risk of more than one trader using the same pseudonym, traders are expected to check for this possibility against all trading pseudonyms that they have heard of.

c) Traders verify other traders' certificates based on their knowledge and recommendations from their trusted peers as detailed later in this section.

d) The trading software that is jointly used by traders to carry out transactions comes from a trustworthy source.

A. The creation of public/private key pairs

Using PGP technology [9, 10], 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. 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. A photograph helps 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 a new self-signed certificate before the existing one expires and then send the newly generated certificate together with their current certificate to any forum members 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.

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

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 [9-11]. 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

A certificate that has been compromised can only be revoked by its owner by performing the following steps:

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

2) Then, 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) Next, send the newly-generated certificate to members of the trading forum prepared 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, multicast a revocation message that is signed by the new and old private keys together with the new and old certificates to other members of the forum. The receiving parties 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.

To assure themselves that identity credentials in a PGP certificate really belong to the party that presents them, a trader can perform the following steps upon receiving a PGP certificate from unfamiliar traders. Some may require further checks depending on the outcome of the check or how careful the recipient is. 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 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.

3) 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 check against an attempt by the subject to spoof another party's identity after discovering that party's private key.

4) Check the photo against their store of certificates to see if that appearance is used with a different identity. This enables the recipient to detect any attempt by the presenting party to be a whitewasher or to create multiple identities.

5) 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 evidence to exclude the presenter from a trading forum's membership for conducting himself inappropriately.

6) 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.

7) Check that the photo appearance is not very similar to that of anyone that there have been broadcast warnings about or about whom an exclusion proposal has been issued. This will give some kind of assurance to the recipient that the certificate is not an alleged malefactor. It would also throw suspicion on the good faith of the signers of the presented certificate.

8) Check that the validity date on the certificate has not expired. An expired certificate doesn't disprove 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 that employs a sanction-backed mechanism will be used as a means to facilitate trust development among traders [3]. An exclusion mechanism [2] that is based on collaborative decision making by a sufficiently large number of forum members is recommended for use to sanction traders that misbehave or have a poor reputation. This will be a strong incentive for traders to behave appropriately especially in fulfilling their transaction agreement and providing truthful deal evaluations and testimonials as they will be open to the risk of being excluded from a trading forum's membership if other traders receive complaint about their misbehaviour

and also an exclusion proposal. 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 will establish a tight binding between a trading party's identity and its reputation.

VII. 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 an 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 threats and attacks that have significant affects on its security. We contend 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 contend that by providing robust identification support, such security threats and attacks can be prevented or at least mitigated.

We have also 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. 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. However, as the attestation process is done totally in a P2P manner among traders without involving any higher certification authority and is based on each attestor's knowledge, identity credentials presented in a PGP certificate that is acceptable to some parties may not be found acceptable to every other party in the trading forum. It will depend solely on the level of trust that the recipients have in the parties that attest the PGP certificate.

We intend that this work together with our proposed group membership service [2] and a reputation system [3] 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. A limitation of this approach is that no implementation has yet been attempted to evaluate its effectiveness. 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.

ACKNOWLEDGMENT

The authors wish to thank the reviewers for their valuable 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 Conference*, 2008, IASK, pp. 223-232.

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

[3] H. Osman and H. Taylor, "Design of a reputation system for m-commerce by ad hoc networking," Technical Report, Dept. of Computer Science, Heriot-Watt University, 2010, pp. 1-7.

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

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

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

[7] 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, pp. 74-77.

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

[9] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume I* 1993. [cited 20/10/09]; Available from: http://www.tinyurls.co.uk/C19930

[10] P. Zimmermann, *Pretty Good Privacy User's Guide, Volume II* 1993. [cited 20/10/09]; Available from: http://www.tinyurls.co.uk/W19931

[11] A. A. Rahman, "*The PGP trust model,*" 1996. [cited 01/07/09]: Available from: http://www.tinyurls.co.uk/H19926 , pp. 1-6.

[12] 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.

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

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

[15] D. S. Thenmozhi and R. Murugan, "Security association in mobile ad hoc networks through self-organized public key certification," *Proc. 4th. Intl Conference on Applied Mathematics and Computer Science*, ACM, 2005. pp. 1-6.

[16] 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.

[17] 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.

[18] 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.