Secure and Private Incentive-Based Advertisement Dissemination in Mobile Ad Hoc Networks

Alexandre Viejo, Francesc Sebé, and Josep Domingo-Ferrer

Rovira i Virgili University
UNESCO Chair in Data Privacy
Department of Computer Engineering and Mathematics
Av. Països Catalans 26, E-43007 Tarragona, Catalonia, Spain
{alexandre.viejo, francesc.sebe, josep.domingo}@urv.cat

Abstract. Advertisement dissemination is a promising M-commerce application which exploits the capabilities of mobile ad hoc networks to increase the visibility of the products being offered by merchants. The starting point is a merchant who generates an advertisement that is subsequently disseminated by citizens who carry mobile devices acting as network nodes. In this paper we present a novel system where users collaborating in offer dissemination are incentivized with e-coin rewards. Our system is proven to be secure and to preserve the privacy of nodes.

Keywords: Advertisement dissemination, Incentive, M-Commerce, Mobile ad hoc network, Privacy, Security.

1 Introduction

In the recent years, e-commerce has become a valid alternative to classic commerce. This has been possible due to the proliferation of home computers equipped with Internet access, cost reduction, special promotions and the possibility of shopping from our home. In spite of its acceptation, e-commerce has not displaced classic shopping which is still the most popular way of trading [1].

New-generation mobile devices (*e.g.* cell phones, PDAs ...) are enabled with wireless communications technologies which paves the way to a broad range of services based on mobile ad-hoc networks (MANET). These networks are formed by mobile nodes which are connected in a self-organized way without any underlying hierarchical infrastructure. In a MANET, nodes not only send or receive but also route data exchanged between other nodes.

The big proliferation of this kind of mobile devices enables the extension of e-commerce (named m-commerce in mobile networks) to traditional shoppers (*e.g.* the users of physical malls). This blurs the distinction between the online and offline worlds and implies the emergence of new trading models which represent new opportunities and challenges.

In this work we present a new m-commerce application based on advertisement dissemination between the nodes of an ad hoc network established in a

A. Miyaji, H. Kikuchi, and K. Rannenberg (Eds.): IWSEC 2007, LNCS 4752, pp. 185–198, 2007.

certain city. In such a system, a merchant generates advertisements related to her products. These advertisements are spread by incentivized volunteers who carry mobile devices and act as network nodes. The high mobility of nodes facilitates the dissemination of advertisements around the city.

Such a system must consider the following aspects:

- Nodes should obtain some reward for disseminating an advertisement. Otherwise, they may refuse to collaborate.
- When incentives for collaborating nodes are established, the system should prevent a malicious node or a malicious collusion of nodes from being able of obtaining higher rewards than due.
- An incentivized system requires accounting the collaboration carried out by nodes. But since a MANET consists of peer nodes operated by users, this accounting information should not allow tracking of users, who should retain their privacy.

In light of the above, an advertisement will contain metadata fields such as the merchant's reward offer per purchase and accounting information corresponding to nodes having collaborated so far in the dissemination of the advertisement. The system ought to be designed so that accounting cannot be maliciously altered but the privacy of the users is guaranteed.

In a MANET, nodes are constantly changing their location. This can cause any pair of nodes to lose direct connectivity any time. In this way, communication systems for MANETs should not depend on centralized authorities that need to be permanently accessible. As to computational capabilities, nodes can be assumed to be able to perform any cryptographic operation.

1.1 Previous Work

There are several proposals in literature which provide incentivized information sharing among mobile devices in a MANET (shared information does not need to be restricted to announcements).

The authors in [5] and [7] propose incentive-based schemes where the network nodes maintain an account with a special node that gives them credit depending on the information they have shared so far. The network nodes can later redeem their credit for money. Nevertheless, both proposals only ensure content integrity. Thus, malicious nodes could claim more credit than they have actually earned.

Providing incentives to intermediate nodes requires a secure way of collecting them. In [4] a lightweight and cheat-resistant micropayment scheme is proposed to stimulate and compensate collaborative peers that devote some of their resources to relay packets for other peers. This scheme focuses on providing a secure and stable channel to exchange data between two peers within an ad hoc network. Intermediate nodes are incentivized to keep this channel operative. However, this work does not address secure dissemination of advertisements across a large set of mobile nodes.

The authors in [6] present AdPASS. This is a system designed to spread digital advertisements among interested mobile nodes in an urban MANET. There are three types of participants in this scheme:

- A *merchant* disseminates digital advertisements within her vicinity. Customer devices learn about advertisements while their customers are browsing around the shop.
- A *customer* device collects advertisements and transmits them to other interested customers while moving around the city. If a customer uses a received advertisement to buy something at the merchant's (the one originating the advertisement), all the users who have co-operated in relaying the advertisement to the buyer receive some bonus points. Such bonus points can later be traded for goods at the merchant's.
- A *mediator* keeps track of the users' accumulated bonus points. The mediator is similar to a central database accessible to both the merchant and the customer. In addition, the mediator acts as an anonymizer to guarantee the anonymity of customers.

AdPASS relies on a *Virtual Bonus Points scheme* to manage the bonus points obtained by a user from dissemination of a certain advertisement. According to this scheme, the merchant initially fixes the total number of bonus points which she is willing to pay for each purchase of the product. Each user who participates in the dissemination decides how many of the remaining bonus points she takes. This decision has an influence on the probability of further dissemination of the advertisement. If a greedy user takes nearly all the bonus points left for a certain advertisement, no other user is likely to be interested in further disseminating the advertisement; this may result in loss of sales opportunities, so a rational user might be expected to take only a fair share of the bonus points allocated per product purchase.

Even though AdPASS is supposed to provide security and privacy to the users who disseminate advertisements, it is not without problems. For one thing, the authors only explain how to get the bonus points but they do not mention how such points are later spent. This issue must be addressed since privacy could be compromised at the time of spending. Besides, this approach requires the users to register with a trusted authority named *mediator* which acts as an *anonymizer* and keeps track of the users' accumulated bonus points. We claim that a good system should not require the presence of a trusted third party (TTP).

On the other hand, the virtual bonus points scheme in AdPASS offers no guarantees of fairness: even though a reasonable behavior can be expected, the fact is that each user disseminating an advertisement can take as many points as she wishes, regardless of how many she actually deserves. Worse yet, collusions are conceivable where colluders exclude other users from dissemination in order to monopolize bonus points. AdPASS must definitely be repaired to thwart those roguish attitudes. Last but not least, the total number of bonus points assigned by the merchant to an advertisement is a *de facto* upper bound on the number of feasible transfers to new disseminators: due to the limited range of MANET

nodes, this implies some limitation in the geographical dissemination range and the sales potential.

To summarize, to the best of our knowledge, none of the existing proposals in the literature addresses all the requirements needed to provide advertisement dissemination through MANETs in an effective, secure and privacy-preserving fashion.

1.2 Contribution and Plan of This Paper

In this work, we present a new scheme designed to disseminate the advertisements of a merchant in mobile ad hoc networks. Our system offers incentives to stimulate the collaboration of nodes. Cryptographic techniques are used to prevent manipulation and preserve the privacy of users. Specifically, the AdPASS [6] system is outperformed in the following aspects:

- Security is achieved against (individual or colluding) dishonest nodes trying to modify transmitted advertisements in order to unlawfully increase their share of incentives.
- Privacy is preserved without resorting to any trusted third party. Our system only requires a certification authority (CA) to certify the merchant's public key. In any case, this authority can not disclose users' identities.
- The incentives rewarding a certain purchase are distributed among all cooperating users given on how long they have held the advertisement leading to that purchase before transferring it to another user. This is a fair proposal which does not restrict the advertisement's dissemination range.

This paper is structured as follows. Section 2 presents some background on public key cryptography over Gap Diffie-Hellman groups. Section 3 describes the new scheme. Section 4 contains a security and privacy analysis. Conclusions are summarized in Section 5.

2 Cryptography over Gap Diffie-Hellman Groups

The construction we propose uses multisignatures over a Gap Diffie-Hellman group [2]. Next, we briefly introduce its mathematical background. A Gap Diffie-Hellman (GDH) group G is an algebraic group of prime order q for which no efficient algorithm can compute g^{ab} for random $g^a, g^b \in G$, but such that there exists an efficient algorithm $D(g^a, g^b, h)$ to decide whether $h = g^{ab}$. GDH groups are suitable for public-key cryptography. The secret key is a random value $x \in \mathbb{Z}_q$ and its corresponding public key is $y \leftarrow g^x$. The signature on a message m is computed as $\sigma \leftarrow \mathcal{H}(m)^x$ ($\mathcal{H}$ is a cryptographic one-way hash function). In the rest of the paper we will denote such a signature on m as $\{m\}_x$. The validity of a signature can be tested by checking $D(y, \mathcal{H}(m), \sigma)$.

GDH groups are convenient to compute multisignatures. Given two signatures of the same message m under two different public keys y_1, y_2, a signature of m under the combined public key $y \leftarrow y_1 y_2 = g^{(x_1+x_2)}$ can be obtained as $\mathcal{H}(m)^{x_1}\mathcal{H}(m)^{x_2} = \mathcal{H}(m)^{x_1+x_2}$.

3 Our Proposal

Our protocol assumes the existence of a merchant and several mobile nodes that communicate through a MANET. We assume the existence of dishonest users (who may act individually or in collusion) interested in obtaining a higher reward than that they are entitled to. We do not require the users to be registered with any central entity. Thus, our system is appropriate for very dynamic environments where connectivity to a central entity may not be guaranteed.

Functionally speaking, a user holding an advertisement actively contacts users within her range and sends them the content of the advertisement. Initially, the advertisement is held by the merchant. Some of the contacted nodes may purchase the advertised good and/or be interested in holding the advertisement themselves for further dissemination.

On the occasion of a purchase request, the buyer sends to the merchant the advertisement (if any) which has motivated her purchase; attaching the advertisement entitles the buyer to a discount. The incentives rewarding that purchase are distributed among the nodes in the path from the merchant to the buyer proportionally to the time they have held the advertisement. E-coins are used to pay those incentives.

In order to facilitate the distribution of incentives, when an advertisement is transferred to a new holder, a time stamp indicating the moment of the transfer is added to the advertisement. In this way, when an advertisement comes back to the merchant together with a purchase request, the merchant can ascertain the incentive that corresponds to each collaborating node. The system is totally anonymous, *i.e.*, the information that nodes add to an advertisement does not allow to identify them. Also, different contributions of a node to different advertisements cannot be related. In this way, unlinkability is also provided. Obviously, we are assuming that the appropriate measures are being taken to avoid node tracking by other means (for instance, frequent change of MAC and IP addresses).

The above system is sustainable for the merchant, who never loses money, because incentives are only paid for advertisements which generated a purchase.

In the following subsections, we describe the protocols and procedures that conform our system. They are:

- Advertisement generation
- Advertisement dissemination
- Advertisement transfer
- Advertisement checking
- Advertisement deposit
- Incentive payment

An advertisement dissemination example in given in Subsection 3.7.

3.1 Advertisement Generation

Merchant M has its public key, PK_M, and its digital certificate issued by a Certification Authority, $Cert_{Aut}\{PK_M\}$. We denote by SK_M the secret key corresponding to PK_M.

1. When M wants to promote a product, it generates an advertisement α containing its public key certificate, the offer description and the expiration time of this offer:

$$\alpha = \{Cert_{Aut}\{PK_M\},\ Description,\ ExpirationTime\}$$

   This advertisement is signed by M to obtain $\{\alpha\}_{SK_M}$.
2. A node U_i interested in disseminating the advertisement contacts M and receives the following message:

$$\beta = \{\alpha,\ PubKeyChain,\ Multisignature,\ TimeChain\}$$

   The fields of β are initialized as follows:
   - $PubKeyChain$ is an ordered list initially left empty;
   - $Multisignature$ is initialized to $\{\alpha\}_{SK_M}$;
   - $TimeChain$ is an ordered list initially containing a single element that is a tuple formed by $Time$ and its signature $\{Time\}_{SK_M}$; $Time$ corresponds to the time this operation has been performed.
3. U_i checks β (see Section 3.4). If all checks are correct, U_i accepts the advertisement from M and starts its dissemination.

3.2 Advertisement Dissemination

Upon accepting an advertisement, U_i informs other nodes about the offer it contains. Due to the inherent mobility in the nodes, U_i is likely to disseminate the offer quite far from M.

Additionally, when U_i contacts a nearby node U_j, U_i asks whether U_j is interested in disseminating the advertisement (our scheme is not linked to any specific framework to perform such initial contact between users, the one presented in AdPASS [6] can be used). If she is, they will start the advertisement transfer. In order to guarantee anonymity and unlinkability, nodes must change their MAC and IP addresses after each contact.

Note that, after an advertisement transfer from U_i to U_j, U_i still holds the advertisement and can continue its dissemination and transfer to other nodes. In this way, the number of nodes disseminating a certain advertisement can grow exponentially.

3.3 Advertisement Transfer

The advertisement transfer protocol requires users U to have a public/private key pair (PK_U/SK_U). To provide unlinkability, this key pair has to be changed after each execution. Before renewing her key pair, a user stores the secret key. This key will be needed in order to receive the incentives (as will be detailed next in Section 3.6).

1. A user U_j interested in an advertisement α held by another user U_i asks U_i to transfer it.
2. U_i appends her public key to the value $PubKeyChain$ in β. This is

$$PubKeyChain' := PubKeyChain \cup PK_{U_i}$$

3. U_i Computes the signature $sig := \{\alpha\}_{SK_{U_i}}$. Then she computes

$$Multisignature' := Multisignature \cdot sig$$

4. U_i obtains the current time, signs it and appends the signed time to the time chain, that is: $TimeChain' := TimeChain \cup \{Time \,||\, \{Time\}_{SK_{U_i}}\}$ (at the end).
5. U_i generates

$$\beta' := \{\alpha,\ PubKeyChain',\ Multisignature', TimeChain'\}$$

and sends it to U_j.
6. U_i stores the secret key SK_{U_i} and generates a new key pair that will be used at the next transfer.
7. U_j checks β' (see Section 3.4). If all checks are correct, U_j informs other nodes about the offer in β'.

3.4 Advertisement Checking

A user U_i receiving a message β should check its validity prior to accepting it. This is done as follows:

1. Check the validity of $Cert_{Aut}\{PK_M\}$ (obtained from α). This requires checking the signature by the authority, its expiration date and, if possible, its revocation status.
2. Compute the product of all public keys contained in $PubKeyChain$ and PK_M. Let us denote by $GlobalKey$ the result of this operation.
3. Check that $Multisignature$ is a correct signature over α that is validated using $GlobalKey$.
4. Check that $ExpirationTime$ (obtained from α) has not expired.
5. Check that the first element of $TimeChain$ is a correct signature generated by the Merchant.
6. For each key contained in $PubKeyChain$, check that the j-th public key in $PubKeyChain$ can validate the $(j+1)$-th signature in $TimeChain$.
7. Finally, check that the values of elements in $TimeChain$ are sorted in ascending order and that the last element corresponds to the current time.

3.5 Advertisement Deposit

A user U_i interested in the product advertised in β contacts the merchant and buys it. By sending β to the merchant, U_i will obtain the price reduction detailed in β. This price reduction motivates users to deposit advertisements.

3.6 Incentive Payment

Once a merchant sells a product to a customer who has deposited an advertisement, it has to pay the incentives to all users who have collaborated in its dissemination.

The merchant gives a fixed amount of money for each received advertisement. This amount of money is divided between collaborating nodes proportionally to the time each collaborating node has held the advertisement along the path from the merchant to the buyer (see Section 3.8 for details about the model used to reward incentives). This information can be obtained from the values in *TimeChain*. The merchant does not know the identity of the nodes that collaborated in the advertisement distribution. It only knows their public key. For each payment the merchant authorizes her bank to issue an e-coin. Let us assume user U_i (who remains anonymous and is only known by her public key) has to receive an e-coin for a given value v.

The merchant sends a message to her bank indicating that she can issue an e-coin with value v to any person providing password p. Then, the merchant publishes a message in a public repository containing p encrypted with the public key of U_i. This indirect procedure through a public repository is needed because U_i is anonymous and may be temporarily out of range.

Later, U_i checks the repository, decrypts the message and obtains p. Using this password, the bank permits her to obtain an e-coin (through the corresponding e-coin issuing protocol). The e-coin system must be anonymous such as the one proposed by Chaum in [3]. This is because the e-coin may later be spent non-anonymously (for instance, if the purchased product has to be delivered by courier). If the e-coin system was not anonymous, it could be possible to link the identity of the person spending the e-coin to the public key used in the dissemination protocol.

3.7 Example of the Protocol

We next clarify the operation of our dissemination protocol following the communication steps described above. We base our explanation on the graphical example shown in Figure 1.

1. Advertisement generation. The merchant wants to promote a certain product and generates an advertisement and informs about it the users within range. User A is interested in disseminating this advertisement and contacts the merchant to request transfer of the advertisement β. Then A checks the validity of β and starts its dissemination. This occurs at time T_0.
2. Advertisement dissemination. A roams around while informing other nodes she meets about advertisement β. Then, A transfers the advertisement to two interested nodes B and D at times T_0+T_1 and $T_0+T_1+T_2$ respectively. At time $T_0 + T_1 + T_3$, node B transfers the advertisement to node C.

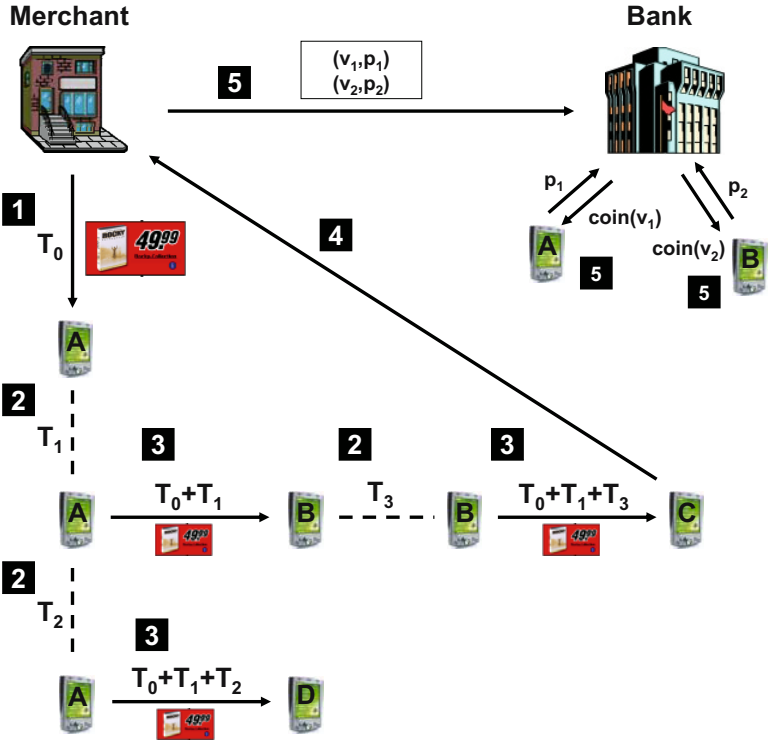

Fig. 1. Graphical example

3. Advertisement transfer. In each transfer, the node which receives the advertisement checks its correctness (see Section 3.4) prior to accepting it.
4. Advertisement deposit. User C is interested in the product advertised in β. Therefore, she contacts the merchant and buys it. By sending β to the merchant, C will benefit from the price reduction detailed in the offer.
5. Incentive payment. The merchant uses the values in the $TimeChain$ embedded in β to determine that A has carried this advertisement during time $T_0 + T_1$ and B has carried it during T_3. Then, the merchant sends a message to its bank indicating that it can issue two e-coins for values $v_1(T_0 + T_1)$ and $v_2(T_3)$ to any person providing passwords p_1 and p_2 respectively. The joint value of those two e-coins is the fixed amount that the merchant is willing to pay for each completed sale of the product. Finally, the merchant publishes p_1 and p_2 encrypted with the public key of A and B respectively in a public repository.

   Later, A and B check the repository and obtain their respective password. Then, they contact the bank and obtain their respective e-coin through the corresponding e-coin issuing protocol.

3.8 Comparison to Other Reward Models

As explained before, in our scheme the merchant divides a fixed amount of money between the nodes which have collaborated in an advertisement dissemination. The money earned by a certain node is proportional to the time which such collaborating node has held the advertisement along the path from the merchant to the buyer. We next explain the advantages of this approach in comparison with the model presented in [6] and with a simple model where each node receives money each time it collaborates (this scheme does not consider how long a node has held the advertisement, only if such node has held it or not).

In [6], the merchant fixes an amount of points as reward to a certain advertisement. Each user which collaborates in the dissemination will claim the number of points that she desires. It means that if a greedy user U_i claims too many points, such advertisement will not be disseminated by any other user since it will not have enough remaining points. Thus, it represents a strong restriction in the advertisement's dissemination range. Besides, users are not rewarded in a fair way and this motivates the users to apply strategies of keeping and passing along points instead of collaborating in the dissemination.

The simple model is more fair than [6]. Each U_i which takes part in a dissemination will receive the same amount of money. However it has two main problems:

1. If there is no limit in the number of hops, also there is no limit in the amount of money that the merchant must give as incentives. It represents a major concern for the merchant. We can solve this problem applying a limit but then the advertisement's dissemination range will be restricted like in [6].
2. Since the merchant gives incentives to each user which collaborates, a certain user with n identities can transfer a certain advertisement to herself $n-1$ times (using her $n-1$ alternative identities). At the end of the process, this user will get incentives for each of her n identities.

To solve these two problems we propose to add a second dimension (the time which a user holds an advertisement) to the simple model. Besides, the merchant establishes a fixed amount of money (incentives) that will be divided between the collaborating users. We next explain how our proposal affects the two problems stated:

1. The merchant after each sale divides the money, assigned to pay advertisement dissemination, between collaborating nodes proportionally to the time each collaborating node has held the advertisement. It means that the merchant never loses money. Besides, users will always receive incentives, although a node which has hold a certain advertisement for a little time in comparison with others, will probably get a very small amount of money.
2. A certain user which holds an advertisement within n epoch (interval of time) will get the same amount of money than a dishonest user which has n different identities and holds the advertisement within 1 epoch with each identity.

4 Security and Privacy Analysis

We next explain the adversary model and the possible attacks the system has to be robust against. We refer to such attacks to prove the security properties achieved by our scheme: integrity, authentication and non-repudiation. We also explain how privacy (anonymity and unlinkability) is obtained.

4.1 Adversary Model

In our system, an adversary is any entity or group of entities wishing to disrupt normal system operation or aiming to collect information on nodes who have collaborated in advertisement dissemination. The nodes that can take part in a dishonest coalition are:

- *The merchant.* It may wish to identify and/or trace nodes who collaborate by spreading announcements. It may also repudiate having generated a certain offer.
- *The bank.* It may wish to identify and/or trace nodes who collaborate in message dissemination.
- *Dishonest users.* They may wish to alter advertisements so as to increase the amount of their assigned reward. They may also wish to inject false disrupting data or identify and/or trace other users.

Possible attacks. On the whole, an adversary can try to perform the following attacks:

- Modify the offer description.
- Repudiate having issued a certain advertisement (when the adversary is the merchant).
- Remove the contribution made by some user to message dissemination.
- Issue a fake advertisement.
- Collect incentives corresponding to other users.
- Obtain the identity of a collaborating node and/or profile her by relating different interactions.

4.2 Attacks and Security/Privacy Properties

Modification of an offer description. This attack refers to the integrity property. Offer descriptions are issued by the Merchant, so we assume it does not take part in the coalition. In our system, an advertisement consists of a message with the following structure:

$$\beta = \{\alpha,\ PubKeyChain,\ Multisignature,\ TimeChain\}$$

The advertisement itself is α which contains its public key certificate, the offer description and its expiration time:

$$\alpha = \{Cert_{Aut}\{PK_M\},\ Description,\ ExpirationTime\}$$

Integrity of the offer description is ensured since α is signed by the merchant (this signature is included in the $Multisignature$ field) and the signature scheme is unforgeable.

Advertisement repudiation. In our scheme, the merchant cannot repudiate having issued an advertisement since it has been signed and the signature on it is verifiable with a certified public key.

Note that, since collaboration in advertisement dissemination is anonymous, users do not need to repudiate having collaborated.

Removal of user contribution to dissemination. Another integrity aspect to be considered is whether users having contributed to the distribution of an advertisement can be unlawfully dropped and forgotten about. Let us assume an advertisement coming from merchant M that has been distributed by users $U_1, U_2, \ldots, U_n$. Let us assume that an intruder wishes to remove U_i from β. The intruder must remove the public key PK_{U_i} from $PubKeyChain$ and remove $\{Time \mid\mid \{Time\}_{SK_{U_i}}\}$ from $TimeChain$. Both removals can be done without any difficulty.

The difficulty for the intruder is to alter the $Multisignature$ field. This field contains the value

$$Multisignature = \mathcal{H}(\alpha)^{SK_M + SK_{U_1} + SK_{U_2} + \ldots + SK_{U_n}}.$$

The intruder must be able to obtain

$$Multisignature' = Multisignature \cdot (\mathcal{H}(\alpha)^{SK_{U_i}})^{-1}$$

Since discrete logarithms are hard to compute in a GDH group, the only way to obtain such value by an intruder is to get the $Multisignature$ field before U_i's contribution. This value can only be obtained if the intruder contacts directly the user who transferred β to U_i. This cannot be done due to the anonymity of the system.

Issuance of a fake advertisement. This attack refers to the authentication property. Our system requires the merchant to sign advertisements using a public key certified by an accepted authority. Generation of a certain advertisement that will be accepted as authentic coming from a valid merchant M, requires knowledge of its private key SK_M. As long as this secret key is not compromised and the signature scheme is unforgeable (a valid signature can only be computed if the secret is known) the system provides authentication and remains secure against this attack.

Collecting incentives from other users. This situation refers to the authentication property too. In our system, E-coins given as incentives can only be collected by the users who have earned them. This is ensured by the incentive payment procedure. During this procedure, the merchant publishes the password required to obtain an e-coin encrypted with a public key whose corresponding

private key is only known by the authentic user. In this way, only the authentic user will be able to obtain this password and request the e-coin.

Disclosure of the identity and/or tracing of users. This attack compromises the privacy of the users. This property consists of two components that must be guaranteed:

- *Anonymity*: Interaction with the system should not reveal the identity of the user.
- *Unlinkability*: It should not be possible to relate different interactions by the same user.

The anonymity of users collaborating in the dissemination of an advertisement is ensured because they simply are requested to provide a public key that does not reveal anything about their identity. Obtaining the password that permits to request an e-coin does not require the user to identify herself either. Finally, an anonymous e-coin system like [3] also provides anonymity when obtaining and spending an e-coin.

Unlinkability is provided if users use a different key pair each time they perform an advertisement transfer. Each user U is able to randomly generate a new public/private key pair (SK_U/PK_U) at will and there is no connection between all the key pairs used by a certain user. Thus, two different public keys from the same user cannot be related by an observer.

5 Conclusions

We have presented a new scheme designed to disseminate advertisements through mobile ad hoc networks. Our scheme outperforms the current proposals in literature by offering security and privacy without requiring the participation of any trusted third party (except for a certification authority that certifies the merchant's public key). In addition to that, we propose a new approach to reward nodes that collaborate in the dissemination according to the time they have been holding an advertisement. Such proposal does not bound the number of transfers for an advertisement (and thus its spreading range) and rewards collaborative nodes with e-coins proportionally to their task.

Disclaimer and Acknowledgments

The authors are solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization. This work was partly supported by the Spanish Ministry of Education through projects SEG2004-04352-C04-01 "PROPRIETAS" and CONSOLIDER CSD2007-00004 "ARES", and by the Government of Catalonia under grant 2005 SGR 00446.

References

1. Euromonitor International. Global Market Information Database (GMID), http://www.gmid.euromonitor.com
2. Boldyreva, A.: Efficient threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-group signature scheme. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 31–46. Springer, Heidelberg (2002)
3. Chaum, D.: Privacy Protected Payments: Unconditional Payer and/or Payee Anonymity. In: Smart Card 2000, pp. 69–92 (1989)
4. Pan, J., Cai, L., Shen, X., Mark, J.W.: Identity-based secure collaboration in wireless ad hoc networks. Computer Networks 51(3), 853–865 (2007)
5. Rajasekaran, H.: An incentive based distribution system for DRM protected content using peer-to-peer networks. In: 1st International Conference on Automated Production of Cross Media Content for Multi-channel Distribution, pp. 150–156 (2005)
6. Straub, T., Heinemann, A.: An Anonymous Bonus Point System For Mobile Commerce Based On Word-Of-Mouth Recommendation. In: Proceedings of the 2004 ACM Symposium on Applied Computing, pp. 766–773 (2004)
7. Vishnumurthy, V., Chandrakumar, S., Sirer, E.: Karma: A secure economic framework for p2p resource sharing. In: Workshop on Economics of Peer-to-Peer Systems (2003)