

Received March 22, 2018, accepted April 29, 2018, date of publication May 8, 2018, date of current version June 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2834359

Motivating Content Sharing and Trustworthiness in Mobile Social Networks

FREDRICK MZEE AWUOR^{1,2,3}, CHIH-YU WANG^{1,2}, (Member, IEEE),
AND TZU-CHIEH TSAI^{1,2,3}, (Member, IEEE)

¹Taiwan International Graduate Program, Social Networks and Human-Centered Computing Program, Institute of Information Science, Academia Sinica, Taipei 11529, Taiwan

²Research Center for Information Technology Innovation, Academia Sinica, Taipei 11529, Taiwan

³Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan

Corresponding author: Chih-Yu Wang (cywang@citi.sinica.edu.tw)

This work was supported in part by the Ministry of Science and Technology under Grant MOST 105-2221-E-001-003-MY3 and in part by the Academia Sinica under the Thematic Research Grant.

ABSTRACT Mobile social networks (MSNs) enable users to discover and share contents with each other, especially at ephemeral events such as exhibitions and conferences where users could be strangers. Nevertheless, the incentive of users to actively share their contents in MSNs may be lacking if the corresponding cost is high. Besides, as users in MSN share contents in an impromptu way as they move, it makes them vulnerable to malicious users who may want to disseminate false contents. This is because users may not have knowledge about the peers they are socially connecting with in the network. In this paper, we propose MCoST, a mechanism that motivates content sharing in MSN and ensures that only trustworthy contents are shared. The mechanism is built on users' collective bidding, content cost sharing, and trust evaluation while guaranteeing individual rationality. MCoST enables content providers to share contents with multiple users simultaneously by utilizing the broadcast nature of wireless transmission. The cost of the content is collectively compensated by the content receivers through the content bidding mechanism in MCoST. In ensuring that users can establish the trustworthiness of their encounters' contents, MCoST incorporates a robust trust evaluation framework that guarantees that content reviews are immutable and tamper-proof, resistive to sybil, and rejection attacks, and that users cannot have multiple and fake identities in the network or reject negative reviews about their contents. This is achieved by integrating a distributed cryptographic hash-chained content review mechanism in the design of MCoST. Performance evaluation shows that the proposed mechanism efficiently evaluates contents' trustworthiness by detecting and discriminating review-chains under sybil or rejection attacks and reduces the time and cost to collect the desired contents by 86% and 40%, respectively, and improves network utilization by 50%.

INDEX TERMS Collective bidding, content reputation, content sharing, hash-chained review, incentives, trust inference, mobile social networks.

I. INTRODUCTION

As smart mobile devices and phones become more ubiquitous and pervasive with wide array of sensors and communication techniques, we can develop mobile social network (MSN) apps that enable these devices to automatically create virtual communities where contents can be shared implicitly. For instance, your smartphone could assist you have a productive encounter with other MSN users by informing you about their interests and valuable contents that they may share with you. Example of such application is Whozthat [1] which uses MSN to enrich offline social interaction among strangers by

suggesting topics of common interest. An exhaustive discussion on structure and design of MSN, and its applications can be found in [2] and [3].

In this paper, we examine the design of MSN to enrich attendees' experience at a large scale exhibition. Exhibition attendees always want to gain insights of new developments in domains of their interests, and to interact with the exhibitors and fellow attendees. Most attendees would wish to visit all the stands and to participate in most activities which fall within their interests. However, as exhibitions run for a short duration (typically 3 – 5 days) with many exhibitors,

these attendees may not be able to visit all the relevant stands whose contents they may be interested in. Besides, it may be costly to individually visit all the stands to assess if their contents are of interest. Nevertheless, we observe that the attendees may wish to discover and connect with their encounters whom they share with similar interests. Also, they may wish to record these offline contacts and transfer them to online social networks such as Facebook for future connections and interactions. This motivates us to utilize the short but frequent encounters at the exhibition to create an MSN as a platform for users to share and exchange their contacts and contents. Such an approach potentially boosts the speed and significantly reduces the cost of content collection.

Notably, MSN users are mostly strangers who wish to discover peers of similar interests and to share contents and contacts in an impromptu way as they move. However, this is at a risk for the MSN users since they may not have knowledge about peers whom they socially connect with. Moreover, MSNs lack central authority, so called trusted third party, who can identify and block malicious users from sharing false contents or malware [4], [5]. Therefore, in enabling impromptu social networking in MSN, there is a need for a mechanism to evaluate trust of unknown users and their contents and to ensure that only trustworthy contents are shared in the network. Trust evaluation in MSN is distributed as each user individually computes trust value of other users and their contents and may share it in the form of content review, so called rating [6]. Thus, a review can be viewed as encounter's opinion of or experience with the user's content and can be used by others to establish the reputation of the content [7], [8]. As MSN lacks trusted authority, content reviews are stored by the content provider who shares them with her encounters who may be interested in the content and thus would wish to infer the content's trustworthiness [9]. This makes reviews susceptible to self-reviews, multiple and fake reviews, and modifications by the content provider.

Exhibition Illustration: Let us consider that user A , B and C are interested in photography and that they have met at stand 9 that is exhibiting on cameras. Further, consider that A is looking for some information on camera deals and offers, while B is looking for cameras that auto-connect to social network apps. Also, consider that C has been to stands 2, 3 and 6 where he collected some contents on drone-cameras and camera deals from company Z . Notably, C has contents that could be relevant to A and thus A may consider to collect them from him during their co-location at stand 9. This way, A saves time that would otherwise have been spent to collect these contents from their respective stands. Nevertheless, C may not have intrinsic motivation to share these contents with A due to the cost he incurred to generate them or the value he attaches to them among others reasons. The cost here refers to the phone resources used to collect and store the content such as energy and memory, and the time and effort involved in collecting the content. Besides, as A and C are most likely strangers who are meeting for the first time during this exhibition, A may need a mechanism to determine

if C 's content is trustworthy. Unless A is able to establish that C is not a malicious user and that his content is genuine, he may be reluctant to collect content from him. We desire to design a system that can motivate users such as C to share their valuable contents with their encounters who may be interested in them while ensuring that his encounters such as A can establish the trustworthiness of the content being shared.

While motivating contents sharing and dissemination in MSN network is preeminent due to the cost incurred to generate contents [10]–[12], it is notable that users may not wish to collect harmful and malicious contents from the network as this would jeopardize their privacy and security. Hence, unless a user can establish that the content being shared is genuine and that the content provider is not malicious, he may not be motivated to collect the content. We first notice that in MSN, both the cost to generate the content and the cost of sharing the content are not known to the content provider's encounters who may be interested in the content. Thus, they may not be able to determine the sufficient compensation that could motivate the content provider to share the content. In addition, the content provider may not know his encounter's valuation of the content that he hosts and hence might not be able to figure out how much the encounter would be willing to pay so as to adjust his price accordingly. Nonetheless, the content can be shared only when the proposed payment by the encounter(s) can sufficiently compensate the cost of sharing the content. We observed that with multiple instances of sharing, the surplus from the sharing transactions could compensate the cost to generate the content. Thus, to increase the sharing rate, we propose a collective content bidding mechanism that motivates users to share their contents with their co-located encounters using a single auction.

During the exhibition, an attendee may be reluctant to use his personal public-private key to sign reviews as this may imperil his privacy since any user in the network who has used his public key to validate his signed review can also use the same key to decrypt his personal contents when they encounter each other. To address this challenge, we consider that exhibition attendees register with the exhibition organizer prior to attending the exhibition. During the registration, the organizer assigns them unique secret codes that they use to generate their individual public-private key pair to use while at the exhibition. This way, only the contents signed using this private key can be decrypted by the user's encounters who have his public key. The reviews are hash-chained to each other and digitally signed by the reviewers using their private keys. This ensures that reviews are undeletable, their integrity is verifiable, and also mitigates the effects of sybil attacks as multiple and fake identities, and self-reviews are easily detectable. In the proposed mechanism, users also share their review history with their co-located encounters which enable them to identify rejection attacks in review-chains of contents that their future encounters may want to share. Thus, in this paper, we propose MCoST, a mechanism

to motivate users to share contents in the MSN network and ensures that the shared contents meet acceptable threshold of trustworthiness. MCoST is built on users' collective bidding, content cost sharing and trust evaluation while ensuring users' individual rationalities. MCoST enables content provider to share content with multiple users simultaneously by utilizing the broadcast nature of wireless transmission. The cost of the content is collectively compensated by the content receivers through the content bidding mechanism in MCoST. In ensuring that users can establish the trustworthiness of their encounters' contents, MCoST incorporates a robust trust evaluation framework that guarantees that content reviews are immutable and tamper-proof, resistive to sybil and rejection attacks, and that users cannot have multiple and fake identities in the network or reject negative reviews about their contents. This is achieved by integrating a distributed cryptographic hash-chained content review mechanism in the design of MCoST. The contributions of this paper can be summarized as follows:

- We formulate and model content sharing problem in MSN networks that ensures that the contents shared in the network meets acceptable threshold of trustworthiness. Using game theory, we establish a content sharing framework that ensures that users have sufficient incentive to share their valuable contents with their co-located encounters. We then derive the optimal content bidding strategy that considers the content's trustworthiness.
- The proposed mechanism incorporates a distributed content trust evaluation mechanism based on cryptographic hash-chained content reviews that is able to detect and be resilient to sybil and rejection attacks. This also ensures that the content reviews are undeletable and resistive to modifications.
- Using simulations, we show that the proposed mechanism efficiently evaluates contents' trustworthiness by detecting and discriminating review-chains under sybil and rejection attacks. We also show that the proposed mechanism could also reduce the time and cost to collect the desired contents in the network by 86% and 40% respectively, and improves network utilization by 50%.

This work is an extension of our initial strategy presented in [13] that focused on incentivizing content sharing in MSN without consideration to the content's trustworthiness. The rest of this paper is organized as follows: Section II reviews related literature, Section III presents the system model while analysis is discussed in Section IV. Trust evaluation framework and performance evaluation are presented in Sections V and VI respectively. Finally, we draw our conclusion in Section VII.

II. RELATED WORK

A. MOTIVATING CONTENT SHARING IN MSN

References [10], [14], and [15] propose incentive schemes for content dissemination in MSN built on virtual rewards and checks that are paid to users who participate in ensuring that the content is delivered to the target receiver. In [11],

contents are disseminated in the network if they are expected to yield high utility in the future. In these schemes [10], [11], [14], [15], the content providers are intrinsically motivated to share and disseminate their contents, for instance advertises in the network. Thus, these schemes are designed to incentivize MSN users to assist the content providers to disseminate their contents to the target recipients. However, in MSNs such as at conferences or exhibitions where users incur costs to generate their valuable contents, the challenge is to motivate the content providers to share their contents with their encounters who may be interested in them. This is one of the problems that we address in this paper.

Generally speaking, MSNs are opportunistic networks built on peer-to-peer (P2P) architecture [2], [10] where users generate contents and share them with their homophylic encounters. This, nonetheless, comes with free-rider problem as most users would want to download much more than they contribute to the network. Besides, users may not be willing to share their contents owing to the values that they may attach to them. Also, sharing contents may make users vulnerable to privacy and security breaches [2]. The mechanism in [16] illustrates that pricing scheme discourages free-riding in opportunistic P2P networks. Service differentiation strategy proposed by [12] and [17] ensures that the amount of content a user can access in the network is proportional to her contribution thus guaranteeing user fairness in the network. Though MSN has close similarity to P2P network, the strategies used in P2P may not be directly applicable to MSN due to their inherent differences. For instance, MSNs are built strictly on selective connection among homophylic encounters. Also, MSNs have ephemeral property as they are formed spontaneously for temporary but specific events. However, since the transmissions in MSN are mostly wireless which can potentially perform multicast, we exploit this property to share the cost of the content among the multiple co-located encounters who are interested in the content.

Considering that MSN is built on smartphones' ability to implicitly generate and share contents, it is noticeable that MSN is similar to participatory mobile-phone sensing. In both, users desire to acquire only contents that meet their preferences from the participants or from their encounters. However, the objective in participatory sensing is to minimize cost of compensating participants [18], [19] such that the proposed payment motivates their participation. In addition, only cost information is private in participatory sensing [19] whereas in MSN, both the content cost and content value are private information. This implies that incentive design mechanisms in participatory sensing may not be directly applicable to promoting content sharing in MSN.

B. CONTENT TRUSTWORTHINESS IN MSN

In [20], social trust framework that limits the maximum number of sybil attacks independent of the network size is proposed. The mechanism is built on user's familiarity with their surrounding peers measured by accumulated time of being in their proximity, and user's similarity with the

encounters. It uses friend ties to build a graph of paired users so as to keep track of user's encounters. Trustworthy service evaluation in MSN is proposed by [8] where service provider independently collects and stores the user reviews about his service and makes these reviews available to users who are interested in his service. This mechanism considers that to submit reviews, users join and register themselves with some groups where the group authority issues them with a bunch of pseudonym secret keys. They use these keys to verify reviews availed by the service provider and to sign their reviews. However, this strategy does not illustrate how these groups are formed or how the group authority is determined, and assumes that the group leader can always be trusted. Thus, should the integrity of the leader be compromised or should he collude with the service provider, the users may never detect. In addition, it also assumes that MSN users are intrinsically motivated to cooperate such that users can submit their reviews through their neighbours in the group which makes this mechanism vulnerable to attacks on trust such as blackhole attack. Moreover, a malicious group leader can submit multiple and fake reviews using the pseudonym secret keys that he stores or give these pseudonym secret keys to the service provider to self review his own service. This could allow the service provider and the group leader to possess multiple fake identities such that their fake reviews would always be disguised as genuine. Besides, the reviews submitted by different groups are not chained or linked together and thus a user may not detect if all the reviews from the previous groups are incorporated in the reviews provided to him. These are among the problems that we address in our proposed trust evaluation mechanism, so called MCoST. In [21], fuzzy trust inference mechanism in MSN is proposed. The mechanism derives user's trustworthiness based on her prestige, familiarity, similarity and risk of trust metrics where prestige is defined as the number of the user's total encounters in the network in comparison to the network size. However, this mechanism does not consider any form of attack on trust. Different from these mechanisms, we propose a cryptographic hash-chained review based trust inference framework that ensures that users cannot have multiple and fake identities in the network and that reviews are immutable, non-deletable and resilient to sybil and rejection attacks.

Due to its one-way and collision resistive property, hash function has been used in security and authentication protocols such as one time password and for authentication between a server and users [22], and to authenticate queries and contents from outsourced databases [23] or web servers [24], [25]. Notably, these mechanisms [22]–[25] are designed for fully connected server based network which is not available in opportunistic ephemeral MSNs that we consider. Thus, these mechanisms may not be applicable to our problem due to the inherent differences in the networks considered. We propose a mechanism that uses a cryptographic hash function to generate hash values to link content's review records so as to produce hash review-chain. The reviewers generate cryptographic signatures on their respective reviews

that can be used by the public to verify the origin, authenticity and integrity of the signed reviews.

While the problem of content trustworthiness in MSN may appear to be an ideal candidate for a typical blockchain algorithm [26]–[30], we notice that the structure and operation of MSN being opportunistic and ephemeral does not permit direct application of blockchain. For instance, blockchain is built on premise of fully connected network [26]–[30] which is missing in MSN as at any given time, users could be connected with co-located peers and thus forming many local but disconnected groups [31] which makes it impossible to validate transactions using the consensus concept in blockchain. Besides, in blockchain networks all the records among users are expected to be similar [26]–[30] such that a user hosting a record that is different from others is assumed to be compromised and untrustworthy. On contrary, same content collected from the same source by different users in MSN are likely to have different review-chains as their encounters will be different [11], [31] and since the network is not fully connected, there is no way each reviewer can report to the whole network when he submits a review to the content host.

Normally, in social networks users opinions and experiences are used by others to deduce the usefulness or quality of a service, product or content offered by a user [7], [8], [32], [33]. These opinions are expressed as reviews or ratings. As these reviews could inform others' decisions about a content or service, it is only essential that they are reliable and trustable. Due to lack of centralized controller in MSN, reviews are susceptible to self-reviews, modifications, and multiple and fake reviewing which could compromise the integrity of reviews and their usefulness in determining the content's quality or trustworthiness. Besides, MSN connections are temporal, spatial-based and users are not fully connected which makes identification of self-reviews or modified reviews difficult. Thus, we propose a mechanism to mitigate trust attacks on content reviews and then derive an algorithm to determine the content's trustworthiness. While security and user privacy in MSN are concerns as shown in [4], [6], and [32], in this study we focus on incentivizing content sharing and guaranteeing that only trustworthy contents are shared in the network. We hope that in our future work, we can leverage our proposed mechanism to address security and privacy issues in MSN.

III. SYSTEM MODEL

A. NETWORK MODEL

We consider an MSN at an exhibition with N users, so called attendees, who collect and share contents with their homophilic co-located encounters. Among these users, we define users who have collected some contents that they would consider sharing with their encounters as agents while users who wish to download contents hosted by agents as principals. During an encounter, agents share the metadata of the contents they wish to share. A content's metadata contains its description and signed reviews from users who

have experienced it. These reviews are hash-chained to form a review-chain to ensure that they are non-modifiable and non-deletable. Exhibition attendees normally form small groups around an exhibit as they listen to the exhibitor and we exploit this co-location to share and disseminate contents among these users. The contact duration during such a co-location is shown in [34]–[36] to be at least 2 minutes but can range to more than half an hour at exhibitions and conferences. Thus, we assume that the contact duration when an encounter occurs is sufficient to exchange content’s metadata, determine the content’s trustworthiness and pricing, and to share the content. The metadata also contains the review history of the agent and those of his previous encounters. A review history is a summary of contents that a user has reviewed in the network and IDs of their providers. A user’s review history is the same for all the content review-chains that he hosts. Even if an encounter is not interested in the content whose metadata has been shared, he will incorporate the peer’s review history into his. This way, he can validate the reliability of a content shared by his future encounter by checking whether the content’s review-chain recorded the reviews that some users reported to have made about the content. This assists in mitigating effects of rejection attacks where content providers would reject negative reviews.

Prior to attending the exhibition, the attendees register with the exhibition organizer who assigns them unique registration codes which the attendees use to generate public-private key to be used to sign reviews while at the exhibition. This way, users sign their reviews using their private keys and make their public keys available in their signed review records to be used by the public to verify the integrity of their reviews and their identities. Though users may have multiple devices while at the exhibition, they all have to be registered using this public-private key pair if they are to be used to collect or review contents in the network. Principal user interested in a content establishes the content’s reputation from its reviews in the review-chain which coupled with similarity and familiarity metrics enables the user to infer the content’s trustworthiness.

We assume that there are K contents in the exhibition and that users can be agents on some contents and principals on other contents. We propose a content sharing framework where users may choose to become agents or principals of certain contents. The decision will depend on their trust evaluation of the content, the cost of the content, and expected profit from the content. We then propose content bidding mechanism, an auction-based strategy that incentivizes agents to share their contents with principals. This is the source of surplus that an agent may collect from principals in the proposed framework. Then lastly, we propose a content evaluation mechanism to assist principals to establish the trustworthiness of the agents’ contents.

B. CONTENT SHARING FRAMEWORK

We first describe the content sharing framework. Normally, at a themed exhibition, attendees are interested in collecting

TABLE 1. Notations and definition.

Notation	Definition
c_k	Cost to generate content k
c_k^D	Cost of sharing content k with interested principals
$p_{i,k}$	i ’s payment (bid) for content k
$\chi_{i,k}$	Measure of i ’s preference for content k
p^*	Optimal bidding strategy
$\pi_{i,k}^t$	Probability that i is a principal for content k at time t
β_i	i ’s threshold for content relevance
K_i^t	Total contents collected by i at time t
$\lambda_{i,j}$	Contact rate between user i and some user j
\mathbf{K}_i	Set of contents user i has collected
$N_{i,k}^t$	Set of principals interested in i ’s content k at time t
$c_{i,s}^t$	i ’s cost at time t to reach exhibitor s
τ_{i,k_j}	i ’s trust inference of j ’s content k

contents that are trustworthy. As MSN has no central authority that can provide reference in regard to trustworthiness of agents and their contents, any principal interested in an agent’s content has to evaluate the trustworthiness of the content by himself. The principal may then share his evaluation as a content review on the content’s metadata to assist the agent’s future principals to evaluate trustworthiness of his content. Let us consider that during an encounter, agent j wishes to share content k with principal i and that i evaluates the trustworthiness of this content to be τ_{i,k_j} . Then we can define i ’s preference for j ’s content k as

$$\chi_{i,k} = \begin{cases} \tau_{i,k_j}, & \text{if } \tau_{i,k_j} > \gamma, \\ 0 & \text{Otherwise.} \end{cases} \tag{1}$$

where γ is the minimum desirable trustworthiness in a content that can be determined empirically as illustrated in Section VI. The derivation of τ_{i,k_j} is discussed later in Section V. (For easy of reference, summary of notations used are defined in Table 1.) If we consider that while at the exhibition, user i is a principal for K_i contents, i.e., he collects K_i contents through his homophylic encounters, then we can derive his utility as

$$u_{prc_i} = \sum_{k \in K_i} (\chi_{i,k} - p_{i,k}) \tag{2}$$

where $p_{i,k}$ is i ’s payment for content k .

C. CONTENT BIDDING MECHANISM

Typically, users may encounter their homophylic peers at stands that are exhibiting on topics of common interest. Thus, we leverage these users’ co-located peers at the stands for content sharing. Specifically, we consider that a user with content to share broadcasts the content’s metadata to her 1-hop neighbors during their co-location at a stand. Users interested in the content respond to the agent within the broadcast’s validity period specified in the metadata. The agent then establishes the number of potential principals interested in the content. This number is broadcasted to the users who responded to the broadcast to assist them establish their optimal bidding strategy. We now assume that a set of principals $N_{i,k}^t$ are interested in agent i ’s content k at time t .

Given their interests and willingness to share the cost to get the content, these principals bid for the content simultaneously. So based on the received bids, agent i decides whether to sell the content to the principals. If agent i decides to sell the content, she broadcasts the content to all the principals in the set $N_{i,k}^t$ and collects the bid from each of them. Similarly, in event that only one user is interested in the content, that is, $|N_{i,k}^t| = 1$, the principal determines his bid accordingly and submits it to agent i who decides whether to sell the content to him.

Assume that principal $j \in N_{i,k}^t$ is interested in content k and proposes to agent i some payment (bid) $p_{j,k}^t$ so as to acquire the content. Let us define c_k^D as the cost to share the content with the interested principals in the set $N_{i,k}^t$. Hence, as c_k^D is the cost to broadcast the content to the principals in the set $N_{i,k}^t$, it can be shared among the $|N_{i,k}^t|$ principals interested in the content. Thus, i shares her content k with $|N_{i,k}^t|$ principals only if $\sum_{j \in N_{i,k}^t} p_{j,k}^t \geq c_k^D$. This way, agent

i ensures that the payment received is at least sufficient to deliver the content to the interested principal(s). Given that MSN is characterized by short but frequent opportunistic encounters, we consider that agent i is able to share content k in T encounters or transactions. Hence we can define the surplus from these sharing transactions of k as

$$\sum_{t \in T} \left(-c_k^D + \sum p_{j,k}^t \right)$$

Then considering that i shares a set \mathbf{K}_i of contents, we can derive his utility as follow

$$u_{agt_i} = \sum_{k \in \mathbf{K}_i} \left(-c_k + \sum_{t \in T} \left(-c_k^D + \sum_{j \in N_{i,k}^t} p_{j,k}^t \right) \right) \quad (3)$$

where c_k is the cost incurred by i to generate content k .

Next, we discuss the best response of a user - in regards to being an agent or a principal for certain contents - when encounter happens. Let us consider that at time t , user i encounters j who has content k from stand s , and that it would cost $c_{i,s}^t$ for i to get to stand s from its current location. Then we can define $\pi_{i,k}^t$, the probability that i would be a principal for agent j 's content k at time t as

$$\pi_{i,k}^t = \begin{cases} 1 & \text{if } p_{i,k}^t < \psi_i^t + \sum_{\kappa \in \mathbf{K}_i^t} \sum_{z \in \mathcal{N}} p_{z,\kappa} < (c_k + c_{i,s}^t), \\ 0 & \text{Otherwise.} \end{cases} \quad (4)$$

where $p_{i,k}^t$ is i 's bid for j 's content k at time t , ψ_i^t is i 's available resource such as phone energy at time t , \mathbf{K}_i^t is i 's total content collected by time t , and $p_{z,\kappa}$ is payment made to i by some principal z who bought his content κ . In (4), user i becomes a principal for content k at time t only if it is cheaper to collect the content from the encounter j than to go to the source stand s and if i has sufficient resource to cater for its bidding strategy, i.e., the proposed payment, $p_{i,k}^t$. Similar to [11] and [37], let us assume that users' encounters

for content sharing follow a Poisson process. Thus, we define contact probability, α_{ij} , between i and j as $\alpha_{ij} = 1 - e^{-\lambda_{i,j}\tau_i}$ where $\lambda_{i,j}$ is contact rate between i and j and τ_i is the total time i spends in the network. Then i 's expected utility can be expressed as

$$u_i = \sum_{t=1}^{\tau_i} \alpha_{ij} \left[\pi_{i,k}^t u_{prc_i} + (1 - \pi_{i,k}^t) u_{agt_i} \right] \quad (5)$$

Then we can formulate network utilization as

$$\Omega = \sum_{i=1}^N \left(\sum_{t=1}^{\tau_i} \alpha_{ij} \left[\pi_{i,k}^t u_{prc_i} + (1 - \pi_{i,k}^t) u_{agt_i} \right] \right) \quad (6)$$

However, for a user i , her goal is to maximize her expected utility. That is,

$$u_i^* := \max \mathbb{E} \left[u_i \left(p_{i,k}^*, p_{j,k}^* \right) \right] \quad (7a)$$

subject to

$$\psi_i + \sum_{k \in \mathbf{K}_i} \sum_{t \in T} \sum_{j \neq i, j \in N_{i,k}^t} p_{j,k}^t \geq \sum_{k \in \mathbf{K}_i} p_{i,k} \quad (7b)$$

$$p_{i,k}, p_{j,k} \geq 0 \quad (7c)$$

where ψ_i is i 's resource when joining the network such as available time, phone energy etc. The constraint (7b) ensures that users' spendings are within their available resources.

IV. ANALYSIS ON CONTENT SHARING

We now analyze the behaviors of MSN users in the proposed content sharing framework. Given that users in the exhibitions are real human and should act rationally to maximize their utility in the framework, we propose to use game theory to analyze their expected behaviors. Let us define a game $G_k = \langle N, (A_{i,k})_{i \in N}, (u_i)_{i \in N} \rangle$ with N players where $A_{i,k}$ is the set of available actions for player i and $a_{i,k} \in A_{i,k}$ is i 's action considering content k while u_i is payoff function of i . Thus, we define the actions of principal i as to bid or not to bidder for content k .

Definition 1 (Nash Equilibrium): $a^* := (a_1^*, a_2^*, \dots)$ is a (pure strategy) Nash equilibrium iff $u_i(a_{i,k}^*, a_{-i,k}^*) \geq u_i(a_{i,k}, a_{-i,k}^*) \forall a_{i,k} \in A_{i,k}$.

Considering that $p^* := (p_{1,k}^*, p_{2,k}^*, \dots, p_{n,k}^*)$ is a Nash equilibrium strategy profile, $p_{i,k}^* \in p^*$ is principal i 's best response if $p_{i,k}^*(\chi_{i,k})$ maximizes her expected payoff $\mathbb{E} \left[u_i(p_{i,k}^*) \right]$ given $u_{-i}(p_{-i,k}^*)$.

The decision of whether to be a principal or an agent for some content k depends on the potential return a user i can get from the content bidding mechanism. Therefore, we need to analyze the bidding strategy of principals in the mechanism. In other words, we need to determine $p_{i,k}^*$ that maximizes i 's expected utility in (7a). Let us consider that $n \subseteq N$ principals have preference $\chi = \{\chi_{1,k}, \chi_{2,k}, \dots, \chi_{n,k}\}$ for agent j 's content k . χ is private information known only by the individual principals and assumed to follow a known distribution that is a common knowledge, i.e. $\chi \sim H = H_1 \times H_2 \times \dots \times H_n$.

Principal i 's bidding strategy $p_{i,k}(\chi_{i,k})$ is a function that maps principal i 's true value $\chi_{i,k}$ to a non-negative payment (or bid) $p_{i,k}$. We consider that $p_{i,k}(\chi_{i,k})$ is strictly increasing and differentiable, and that $p_{i,k}(\chi_{i,k}) \leq \chi_{i,k}$ for all $\chi_{i,k}$. (For ease of notation, we drop k and simply write $p_{i,k}(\chi_{i,k})$ as $p_i(\chi_i)$ to mean principal i 's proposed bid to agent j for its content k .) Let us assume that i 's valuation $\chi_i \sim U(0, 1)$. This implies that $p_i \sim U(0, 1-a)$ where $a \in [0, 1]$. The objective of principal i is to maximize its expected utility $\mathbb{E}[u_{prc_i}(p_i) | \chi_i]$, that is,

$$\begin{aligned} & \max \Pr(i \text{ obtains content } k) \times (\chi_i - p_i) \\ & = \max \Pr\left(\sum_{i \in N_{j,k}^t} p_i \geq c_k^D\right) (\chi_i - p_i) \quad (8) \end{aligned}$$

1) CASE THAT $|N_{j,k}^t| = 1$

That is, only 1 co-located encounter is interested in agent i 's content k . This implies that $\sum_{i \in N_{j,k}^t} p_i = p_i$ and thus (8) is

equivalent to

$$\max \Pr(c_k^D \leq p_i) (\chi_i - p_i)$$

However,

$$\begin{aligned} \Pr(c_k^D \leq p_i) & = 1 - \Pr(c_k^D > p_i) \\ & = 1 - \left[1 - \Pr(c_k^D < p_i)\right] \end{aligned}$$

Considering that c_k^D is distributed according to $U[0, 1]$, $1 - [1 - \Pr(c_k^D < p_i)]$ can be simplified to $1 - [1 - p_i] = p_i$. Thus, (8) can be expressed as

$$\max p_i (\chi_i - p_i)$$

Differentiating $p_i (\chi_i - p_i)$ w.r.t p_i and setting to 0 gives

$$p_i^* = \frac{1}{2} \chi_i \quad (9)$$

Hence (9) is the optimal bidding strategy that maximizes the expected utility in (8) when $|N_{j,k}^t| = 1$.

2) CASE THAT $|N_{j,k}^t| > 1$

Letting $|N_{j,k}^t| = n$, we can write (8) as

$$\begin{aligned} & \max \Pr\left(\sum_{m \in n} p_m \geq c_k^D\right) (\chi_i - p_i) \\ & = \max \Pr\left(\sum_{m=1}^{n-1} p_m \geq c_k^D - p_i\right) (\chi_i - p_i) \quad (10) \end{aligned}$$

Let us define a random variable $Y = \sum_{m=1}^{n-1} p_m$. Then by definition, Y is Irwin-Hall (uniform sum) distributed with pdf

$$f_Y(y; n-1) = \frac{1}{\tilde{a}(n-2)!} \sum_{m=0}^{\lfloor \frac{y}{\tilde{a}} \rfloor} (-1)^m \binom{n-1}{m} \left(\frac{y}{\tilde{a}} - m\right)^{n-2}$$

where $\tilde{a} = 1 - a$.

Thus,

$$\begin{aligned} \Pr(Y \geq c_k^D - p_i) & = \int_{c_k^D - p_i}^{\infty} f_Y(y; n-1) \partial y \\ & = 1 - \Pr(Y < c_k^D - p_i) \\ & = 1 - \frac{1}{(n-1)!} \sum_{m=0}^{\lfloor r \rfloor} (-1)^m \binom{n-1}{m} (r-m)^{n-1} \end{aligned}$$

where $r = \frac{c_k^D - p_i}{\tilde{a}}$.

Let

$$z = \sum_{m=0}^{\lfloor r \rfloor} (-1)^m \binom{n-1}{m} (r-m)$$

then i 's expected utility in (10) can be written as follows

$$\left(1 - \frac{1}{(n-1)!} z^{n-1}\right) (\chi_i - p_i)$$

Taking first order derivative w.r.t p_i and setting to 0,

$$\frac{\partial}{\partial p_i} \left(\left(1 - \frac{1}{(n-1)!} z^{n-1}\right) (\chi_i - p_i) \right) = 0$$

and

$$(\chi_i - p_i) = \frac{\tilde{a}(n-2)!}{z^{n-2}} - \frac{\tilde{a}z}{n-1}$$

Hence i 's optimal bidding strategy, p_i^* , that maximizes the expected utility in (8) when $|N_{j,k}^t| > 1$ is

$$p_i^* = \chi_i - f(p_i) \quad (11)$$

where $f(p_i) = \frac{\tilde{a}(n-1)! - \tilde{a}z^{n-1}}{(n-1)z^{n-2}}$.

Recall that $\chi_i \sim U(0, 1)$ and $p_i \sim U(0, 1-a)$, thus, $\chi_i - p_i = 1 - (1-a)$ and hence $\chi_i - p_i = a$. Combining this argument with $\chi_i - p_i = f(p_i)$ derived in (11), it follows that $f(p_i) = a$. However, (11) is not in closed form and thus we employ numerical approximations to estimate the range of values of variables in $f(p_i)$. In these simulations, we search for the values of $f(p_i)$ such that for different values of a , c_k^D and n , $f(p_i)$ is approximately equal to a . We then use these estimations to determine the user's optimal bidding strategy. The results are shown in Fig 1. From the numerical approximations, the range of these variables are: $0 \leq p_i \leq (1-a)$, $f(p_i) \cong a$, $0.1 \leq c_k^D \leq 1.0$ and

$$a = \begin{cases} 0.5 & \text{if } n = 2, \\ 0.55, \dots, 0.57 & \text{if } n = 3, 4, \dots, 50, \\ 0.58 & \text{Otherwise.} \end{cases} \quad (12)$$

To this end, we derive the collective content bidding and cost sharing mechanism in Algorithm 1. The main outline of the algorithm is that users in the network explore the exhibition by visiting exactly one stand in each timeslot. Besides, they can only visit stands whose contents they have not collected or accessed. While at the stands, users are able to collect contents from both the exhibitor and their co-located

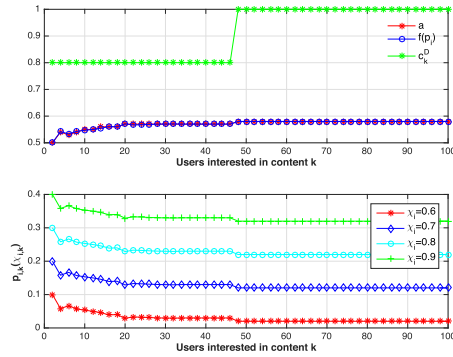


FIGURE 1. Bidding strategy.

Algorithm 1 Content Sharing Mechanism Using MCoST

```

1:  $ngb(i)$ : Set of  $i$ 's 1-hop neighbors
2:  $ngb_k(i) = \{\}$ : Set of  $i$ 's 1-hop neighbors interested in his
   content  $k$ 
3:  $princ_k = 0$ ;  $sumbid_k = 0$ : Counters
4: procedure Content Sharing
5: if  $i$  wishes to share his content  $k$  then
6:    $i$  broadcasts  $k$ 's metadata to  $ngb(i)$  at the stand;
7:   while broadcast is valid do
8:     for  $j = 1$  to  $|ngb(i)|$  do
9:        $j$  decides to collect  $k$  from  $i$  based on (1) and (4);
10:      if  $\left(\left(\pi_{j,k}^t > 0\right) \&\& \left(\chi_{j,k} > 0\right)\right)$  then
11:         $j \in ngb(i)$  sends WANT message to  $i$ ;
12:         $princ_k += 1$ ;
13:         $ngb_k(i) = ngb_k(i) \cup j$ ;
14:      end if; end for; end while
15:      if  $(princ_k > 0)$  then  $i$  broadcasts  $princ_k$  to  $ngb_k(i)$ 
16:        for  $j = 1$  to  $|ngb_k(i)|$  do
17:          if  $(princ_k == 1)$  then
18:             $j \in ngb_k(i)$  determines  $p_{j,k}$  according to (9);
19:          else  $j \in ngb_k(i)$  determines  $p_{j,k}$  using (11);
20:            end if
21:             $j$  submits its bid,  $p_{j,k}$ , to  $i$ ;
22:             $sumbid_k += p_{j,k}$ ;
23:          end for; end if
24:          if  $(sumbid_k \geq c_k^D)$  then
25:             $i$  broadcasts content  $k$  to  $ngb_k(i)$ ;
26:             $j \in ngb_k(i)$  submits payment  $p_{j,k}$  to  $i$ ;
27:          end if; end if
28: end procedure

```

encounters. Users who wish to share their contents broadcast the metadata of these contents to their 1-hop neighbors co-located at the stand. Users decide to request for contents whose metadata are shared based on (1) and (4). The content owner, so called agent, then broadcasts the number of users interested in his content to his co-located peers who had responded to the broadcast of the content's metadata. This assists these principals to determine their bids for the content which they then submit to the agent. The agent broadcasts

the content to these principals if the sum received bids is at least sufficient to meet the cost of content sharing. The principals then make their payments once the agent has shared the content.

V. CONTENT TRUSTWORTHINESS

We now discuss how we establish and evaluate the trustworthiness of contents in the proposed framework. Recall that the utility of a user depends on his content's trustworthy and that user's encounters evaluate the content's trustworthiness individually due to lack of trusted authority that can be used to provide central reference to the user's content. But since user's encounters share their experience of the content in form of content reviews, we can leverage these reviews to establish the content's reputation which combined with other metrics such as similarity and familiarity can assist user's future encounters to evaluate the content's trustworthiness during the exhibition. However, reviews are vulnerable to sybil and rejection attacks and thus we propose to use a cryptographic hash-chained approach that makes reviews non-deletable and resistant to modifications.

Content's metadata contains the content provider's review history and the hash-chained reviews of the content from users who have experienced it. The first record stores the review history (rh) while the second record stores the identity, so called public key, of the content provider and the description of the content. The subsequent records in the metadata contain the reviews. The rh record is linked to the second record while the second record and all the subsequent records are hash-chained to each other. Basically, rh record stores the ID of all contents reviewed by the user and his previous encounters, and the content providers of those contents. These details are captured in the reviewer ID (RID), content ID (CID) and content provider ID (CPID) fields. (For the sake of clarity, we also refer to metadata as review-chain.) All contents' metadata from a user have the same rh information. During the opportunistic encounters, users share the metadata of contents they wish to share with their co-located peers. They then update their own rh records with the new rh information from these encounters. For instance, consider that user 1 and 2 have collected and reviewed contents x and c provided by user 7 and 9 respectively. When user 1 encounters user 2, they will share and update their rh records accordingly and both will have rh record as in Fig. 2. Consequently, when a user is interested in a content whose metadata is shared, he first checks if the content's review is detailed in his rh record. If it exists, he checks that all the reviews about this content captured in his rh record to have been submitted to this content provider are all present in the content's review-chain. If any of the reviews is missing then it implies that this content provider rejected the review probably because it was a negative review that would discredit the content's reputation. Such a review-chain is considered as not reliable as it is under rejection attack.

Besides the rh record, all other records in the review-chain contain five fields, that is; the review record number, reviewer

Record #: 0000		
RID	CID	CPID
User1	X	User7
User2	C	User9

FIGURE 2. Review history.

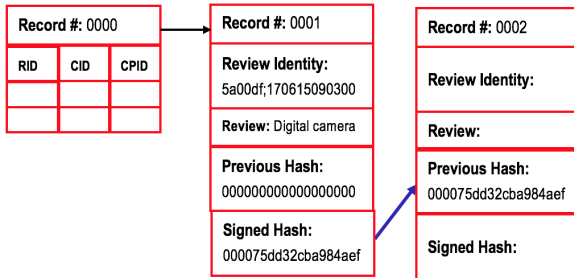


FIGURE 3. Content description.

identity, review entry, signed hash value and previous review record’s hash value as shown in Fig. 3. The review record number shows the index of the record. The reviewer identity captures the public key of the reviewer and the time-stamp when the review record was signed. The review is stored in the review entry field. The signed hash value contains the signed review record’s hash value while the previous hash value field contains the hash value of the previous review record and it is chained to the current review record. Let us define the review record message as the review entry and previous review record’s hash value. So the content reviewer digitally signs the review record’s message using his private key to generate the review record’s signed hash value. This automatically captures the reviewer’s public key and the time-stamp when the review message is signed. It also creates a new and empty review record that is hash chained to the current review record. Subsequent review is submitted using this empty review record as illustrated in Fig. 3. That is, user i registers with the exhibition organiser and is assigned a unique code reg_i that he uses to generate its public-private key pair (pk_i, pt_i) to use to encrypt and decrypt his reviews while at the exhibition. He uses the private key pt_i to sign his reviews and avails his public key pk_i in the review to be used by the public to verify his signature. In other words, i generates the hash value for a review message as $h_i = sign_{pt_i}(review_message)$ while any user can verify i ’s signature using $h'_i = verify_{pk_i}(review_message)$ and can conclude that the review is compromised if $h'_i \neq h_i$.

Let us consider Figs. 3 and 4 to illustrate the operation of MCoST. The review-chain record indexed 0000 is the rh record of this content provider while the second record, so called genesis record, indexed 0001 stores the content’s description and the public key of the content provider, i.e., $5a00df$, which can be used to verify its signed hash value. The reviewer identity field also contains the time-stamp

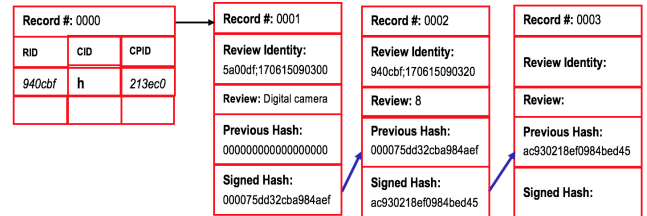


FIGURE 4. Review-chain with 1 review.

when the review record was signed, i.e., 170615090300 - 15th June 2017 at 9.03 am. The moment this review record is signed by the content provider, an empty review record indexed 0002 is automatically created that is hash chained to this genesis review record. So this becomes the content’s metadata that the content provider shares with his co-located peer who may be interested in the content. Let us consider that some user identity public key $940cbf$ is interested in this content. First, user $940cbf$ updates his rh record with entries in that of $5a00df$. Next, $940cbf$ checks if there is any review entry in his rh record that other users reported to have submitted to $5a00df$ about this content. If there is, then $940cbf$ checks if the review is captured in the review-chain shared by $5a00df$. User $940cbf$ concludes that $5a00df$ ’s review-chain is unreliable if any review entry about this content recorded in $940cbf$ ’s rh record to have been submitted to $5a00df$ is omitted in $5a00df$ ’s review-chain. Otherwise, $940cbf$ performs the next step which is to verify that all review records in the shared review-chain are signed, and that no malicious user has made any multiple reviews in it. $940cbf$ also verifies that there are no self-reviews from $5a00df$ in the review-chain by searching for any review record which has $5a00df$ ’s public key besides the genesis record. Finally, $940cbf$ then computes the trustworthiness of the content (as derived later in (16)) and decides to bid for the content if its trust inference is acceptable as defined in (1).

Assume that $940cbf$ gives this content a rating of 8. He then generates the cryptographic hash value of the review record message. Next, he digitally signs this hash value using his private key to generate the review record’s signed hash value which in effect captures his public key and the time-stamp of the record signing. This also generates a review record indexed 0003 which is hash chained to this current review record 0002 as illustrated in Fig. 4. This becomes the content’s new review-chain which $940cbf$ sends to the content provider $5a00df$ to replace the review-chain he previously held. Both $5a00df$ and $940cbf$ shares this new review-chain with their subsequent encounters who may be interested in this content. If we consider that $5a00df$ later encounters and shares this content with $fb954$ who gives the content a rating of 4, then $5a00df$ ’s review-chain would look like Fig. 5.

A. DETECTING SYBIL AND REJECTION ATTACKS

The review-chain needs to ensure that it is resistive to the effects of sybil attacks since MSN lacks trusted authority

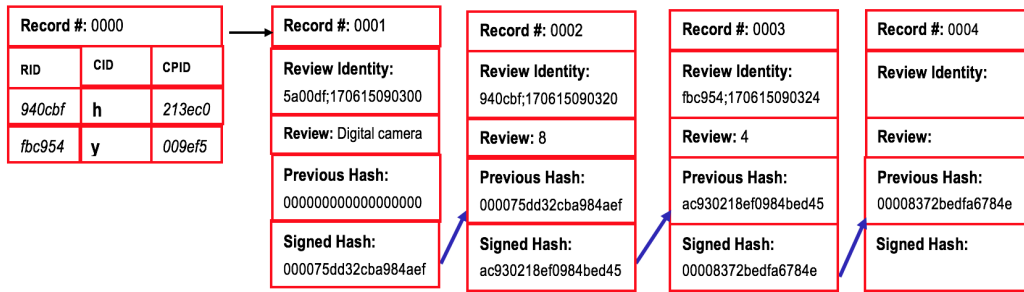


FIGURE 5. Review-chain with 2 reviews.

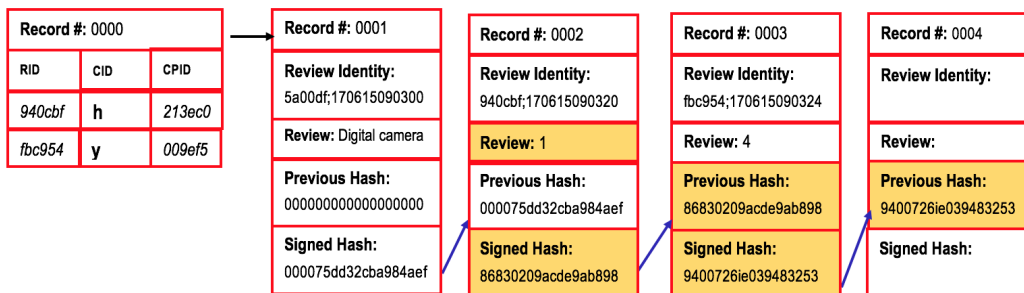


FIGURE 6. Sybil attack.

to keep track of updates on contents’ review-chains or to authenticate users in the network so as to identify and block malicious users. Similar to [8] and [20], we define the following potential attacks on reviews:

Sybil attack 1: Multiple reviews that occur when malicious content providers collude with their cronies to submit multiple positive reviews to promote the reputation of their contents. This attack also occurs when malicious users intentionally submit multiple negative reviews to discredit the reputation of their foes’ contents.

Sybil attack 2: Self-reviews where content providers modify negative reviews in their own contents’ review-chains to positive reviews so as to boost the reputation of their contents.

Rejection attack: This occurs when a user submits a negative review and the content provider silently rejects or drops it. Normally, the content provider would update the previously held review-chain with the new one containing the encounter’s review. However, in this case, the content provider fails to update his previously held review-chain to avoid having reviews that could lower the reputation of his content. In MSN where user encounters are opportunistic, future encounters of this content provider may never know that he rejected a negative review submitted to his content’s review-chain.

These attacks compromise the integrity and reliability of content reviews and thus mislead users about the reputation of a content such that malicious contents may be perceived as trustworthy while genuine contents perceived as untrustworthy.

In designing MCoST, we assume that users acquire only contents that they have not collected from the network and submit one reviews for each content collected. Thus, a user who submits multiple reviews in the same review-chain is considered malicious. Let us consider that a malicious user decides to change the review entry of review record index 0002 from 8 to 1. This will change the signed hash value of review record 0002 and the hash values of all the subsequent review records in the review-chain as shown in Fig. 6. Any user who receives this review-chain can verify that its integrity has been compromised as the public key of the reviewers in the review records 0002, 0003 and the subsequent records would not match their respective signatures in the signed hash value. This makes this review-chain invalid. Nonetheless, a content provider may consider rejecting a review-chain with negative review from his encounter. To illustrate how MCoST mitigates this form of attack, let us consider that user 2 in Fig. 2 is not interested in content x shared by user 1 but nonetheless updates his rh record with that of user 1 as discussed earlier. Assume that user 2 soon after encounters user 3 who updates his rh record with that of user 2. Later, user 3 encounters user 7 whom user 3 is interested in his content x . However, from user 3’s rh record, he knows that user 1 had reviewed content x provided by user 7. So user 3 verifies if user 1’s review is captured in content x ’s review-chain shared by user 7. If user 7 had rejected user 1’s review, user 3 will notice that it is missing in the review-chain and this would imply that this review-chain is under rejection attack and thus not reliable.

Algorithm 2 Reputation of a Content’s Review-Chain

```

1:  $l$ : length of content  $k$ 's review-chain
2:  $cont_k$ : provider of content  $k$ 
3:  $rh$ : review history of a user interested in content  $k$ 
4:  $status = 1$ ; validity of content's review-chain
5: procedure ContentReputation
6: if  $k > 2$  then
7:   if content  $k$ 's entry exist in  $rh$  under  $cont_k$  then
8:     Identify the reviewers of content  $k$  in  $rh$ 
9:   if any reviewer is missing in content  $k$ 's review-chain
     then
10:      $status = 0$ ; \textit{\textbackslash}rejection attack exists
11:     break; end if; end if
12:   for  $i = 3$  to  $l$  do
13:     if record( $i$ ) is NOT signed then
14:        $status = 0$ ; \textit{\textbackslash}review is tampered with
15:       break; end if
16:     message=[review( $i$ ),previous_hash_value( $i$ )];
17:     temp_message=[verify(public_key( $i$ ),
       hash_value( $i$ ))]
18:     if message != temp_message then
19:        $status = 0$ ; \textit{\textbackslash}integrity of review compromised
20:       break; end if
21:     if revieweridentity(2)==revieweridentity( $i$ ) then
22:        $status = 0$ ; \textit{\textbackslash}self-reviewing exist
23:       break; end if
24:     for  $j = 2$  to  $k$  do
25:       if revieweridentity( $i$ )==revieweridentity( $j$ ) then
26:          $status = 0$ ; \textit{\textbackslash}multiple reviews exist
27:         break; end if; end for
28:     end for; end if
29:     if  $status == 1$  then
30:       Content's review-chain is valid
31:       Determine reputation score according to (13)
32:     else
33:       Reputation score = 0
34:     end if
35:   end procedure

```

B. ESTABLISHING REPUTATION AND TRUSTWORTHINESS OF A CONTENT

A review-chain is considered reputable if it is void of both sybil and rejection attacks. Using Algorithm 2, a user’s encounters are able to verify the integrity of his content’s reviews and to determine its reputation. Algorithm 2 detects review-chains whose integrity are compromised due to sybil or rejection attacks and classifies them as non-reputable, and assigns them 0 score in regard to reputability. Given that users wish to collect only contents whose review-chains are reputable, we need to establish a mechanism to determine the reputation score of such contents. Define t_m as the time when a user encounters content provider of content m and t_k as the time when review record k in m 's review-chain was signed. Then the age of k at the time of encounter

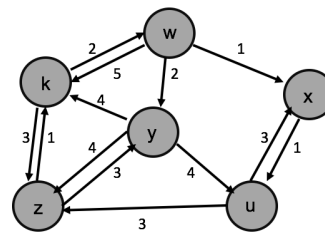


FIGURE 7. User encounter.

is $t_m - t_k$. Consider that a content reviewer gives a rating r , where $r \in [r_{min}, r_{max}]$ and $0 \leq r_{min} \leq r_{max}$. Also, let reviewer’s rating for the content captured in record k be r_k . Then we can compute the reputation score, RS_m , of content m from its review-chain as follows

$$RS_m = \frac{1}{\kappa} \sum_{k=1}^{\kappa} \frac{r_k}{r_{max}} \left(1 - e^{-\frac{1}{t_m - t_k}} \right) \quad (13)$$

where κ is total reviews in m 's review-chain. In (13), $\left(1 - e^{-\frac{1}{t_m - t_k}} \right)$ has the property of inverse sigmoid function to ensure that reviews are weighted based on their ages in the review-chain. This effects the time decay property of trust. r_{max} normalizes the expected reputation score to $0 \leq RS_m \leq 1$.

In social networks, users who tend to interact often can be considered to trust each other as they are assumed to be familiar with each other [20], [21], [32], [38]. In consideration to MSN, we can explore users’ previous content sharing interactions to determine their familiarity. Consider a weighted and directed content sharing interaction graph in MSN defined as $G = (V, E)$ where V is the set of users and E denotes edges defined as interactions between users and weighted by the number of content sharing interactions as shown in Fig. 7. Specifically, each content sharing is considered as an encounter and thus the weights on inbound edges are the number of interactions where the user acquired content from the given content provider. Define $N_G(k) = \{v \in V_G | v, k \in E_G\}$ as the set of k 's neighbours that k has acquired contents from at least once, then we can derive k 's familiarity score for its encounter v as follows

$$FS(k, v) = \begin{cases} \frac{E_G(v, k)}{\sum_{i \in N_G(k)} E_G(i, k)} & \text{if } v \in N_G(k), \\ 0 & \text{Otherwise.} \end{cases} \quad (14)$$

where $E_G(v, k)$ is weight of inbound edge from v to k , and $0 \leq FS(k, v) \leq 1$. For instance, in Fig. 7, $FS(z, y) = \frac{E_G(y,z)}{E_G(k,z)+E_G(u,z)+E_G(y,z)} = \frac{4}{3+3+4} = 0.4$. Eq. (14) captures the view that users give much consideration to contents from encounters whom they have previously collected most contents from.

Generally speaking, in social networks users tend to trust their peers who are similar to them [3], [20], [21] and in consideration to MSN, this implies that users can trust

their encounters if they have similar user profiles or interests [31], or if they have common encounters. Thus, let us consider that k would wish to acquire content m from his encounter v . So he examines if he has interacted and acquired content from any of the reviewers in content m 's review-chain. Let us define $R_m(v)$ as the set of users who have reviewed v 's content m that k is interested in, then we can derive similarity score based on common encounters, SC , using Jaccard similarity coefficient [3] as

$$SC(k, v) = \frac{|N_G(k) \cap R_m(v)|}{|N_G(k) \cup R_m(v)|}$$

This enables k to determine the fraction of his encounters who have acquired content m which generally measures content m 's trustworthiness within k 's trusted encounters. Next, let us also consider that a user's profile vector is constructed from the keywords that she uses to describe her profile and interests. Then we can use cosine metrics [3], [39] to distinguish how similar a user's profile vector is to another. Let $\vec{s}_k = (s_k^1, s_k^2, \dots)$ be a vector describing user k 's profile and interests and $\vec{s}_v = (s_v^1, s_v^2, \dots)$ describe that of content provider v whose content user k is interested in. Then the similarity of k and v , $sim(k, v)$, can be derived using cosine metrics as follows

$$sim(k, v) = \frac{\vec{s}_k \cdot \vec{s}_v}{\|\vec{s}_k\|_2 \|\vec{s}_v\|_2}$$

where $-1 \leq sim(k, v) \leq 1$. $sim(k, v) = -1$ means that k and v are exactly opposite, $sim(k, v) = 1$ means that they are exactly the same and 0 implies that they are decorrelated. Hence we can derive similarity score based on profile and interests, SP , as

$$SP(k, v) = \begin{cases} sim(k, v) & \text{if } sim(k, v) > 0, \\ 0 & \text{Otherwise.} \end{cases} \quad (15)$$

The argument presented in (15) is that since users tend to trust their friends and normally friends tend to have similar interests and profiles, then it follows that contents from encounters with similar profiles or interests to the user can as well be trusted by the user. Finally, the similarity score between k and v , $SS(k, v)$, can be formulated as

$$SS(k, v) = \lambda SP(k, v) + (1 - \lambda) SC(k, v)$$

where $0 \leq \lambda \leq 1$ and λ is system parameter that can be determined empirically. Setting λ close to 1 enables the user to give more attention to contents from peers with similar profile or interests to hers while setting λ close to 0 enables her to focus on contents that are trusted by her previous encounters.

To this end, user k can infer the trustworthiness of content m provided by user v using (16)

$$\tau_{k,m_v} = \alpha RS_m + (1 - \alpha) [\beta SS(k, v) + (1 - \beta) FS(k, v)] \quad (16)$$

where α and β are system parameters associated with MSN application and $0 \leq \alpha, \beta \leq 1$. In (16), significant contribution is assigned to the content's reputation to ensure

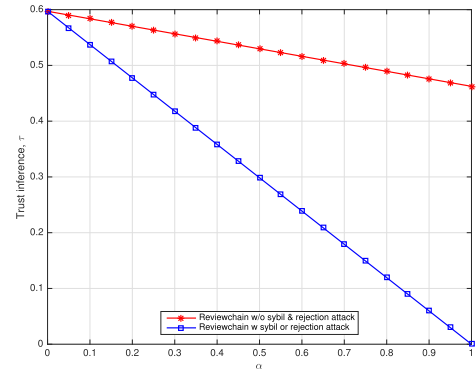


FIGURE 8. Effect of α on trust inference.

TABLE 2. Simulation parameters.

Parameter	Value
α : shading factor	[0.5, 0.58]
c_k : cost to generate content k	0.5
c_k^P : cost of sharing content k	[0.1, 1.0]
User's transmission range	15m
Contents of interest in the network	50

that contents whose review-chains are compromised cannot be disguised as genuine. Thus, setting α close to 1 enables a user to focus on collecting contents that are considered reputable as is illustrated in Fig. 8. The choice of β allows the user to decide whether to give more attention to contents from familiar or similar peers. For instance, setting β close to 0 enables the user to focus on contents from familiar users. k can then use τ_{k,m_v} to determine his preference for content m as described earlier in (1).

VI. PERFORMANCE EVALUATION

A. SIMULATION SETUP

For simulation, we consider an exhibition area of $250m - by - 250m$ with 200 exhibition attendees that are uniformly deployed in the area. In every timeslot, attendees are assumed to visit stands whose contents they have not collected or accessed. While at a stand, users share contents with their co-located 1-hop neighbors. The contact duration (that is, length of each timeslot) is set to 3 minutes [34]–[36]. The probability that a user is a principal for a certain content while at the stand is either 0 or 1 according to (4) while the contact rate is set to 0.33 similar to [37]. Users' mobility are considered to follow random waypoint model where users move in random destinations at a speed uniformly distributed in [0.5, 1.5] m/s. Other simulation parameters are set according to (12) as shown in Table 2.

The reviews on content, so called ratings, are assumed to be uniformly distributed in $[r_{min} = 1, r_{max} = 10]$. We consider that users describe their profiles a prior to joining the network using a set of predefined keywords. The pool of keywords consist of 25 different keywords and a user can select a maximum of 5 keywords that closely describes his interests or profile. Then we use these keywords to build

user's profile vector. We consider that users are interested in both the contents trusted by their previous encounters and contents provided by users similar to them. Hence we set $\lambda = 0.5$. We also consider that users are interested in contents from encounters whom they are both similar and familiar with, and thus we set $\beta = 0.5$. In view of (16), setting α close to 0 makes contents whose review-chains are under attack indistinguishable from those with genuine review-chains. However, this enables the user to give more attention to contents from encounters whom she is both similar and familiar with. Conversely, setting α close to 1 enables the user to give more attention to content's reputation and less consideration to her similarity or familiarity with the content's provider. This trade-off is illustrated in Fig. 8. Thus in this simulation, we set $\alpha = 0.5$ so as to pay equal attention to both the content's reputation, and user's familiarity and similarity with the content's provider.

To illustrate the performance of MCoST under sybil attack, we consider three forms of sybil attacks. That is, sybil attack 1 where content provider colludes with his cronies in the network to submit multiple and fake high ratings about his content so as to promote the content's reputation; sybil attack 2 where foes of the content provider make multiple and fake reviews with low ratings to discredit his content's reputation; and sybil attack 3 where the content provider self reviews his content by modifying low ratings to high ratings so as to boost the reputation of the content. We consider that under sybil attack 1 and 2, content provider's cronies and foes submit multiple and fake reviews of rating r_{max} and r_{min} respectively. Under sybil attack 3, the content provider modifies all reviews which are below r_{ths} to r_{max} where $r_{ths} = \frac{1}{2}(r_{min} + r_{max})$. In the case of rejection attack, we consider that the content provider rejects all reviews which are less than r_{ths} .

For comparison, we define two baseline algorithms, i.e., Single-1 and Group-3. In Single-1, exhibition attendees collect contents by physically visiting all the stands. This way, the attendee is compelled to individually visit each stand, examine the relevance of its content and then decide whether to collect the content. Thereafter, the attendee moves to the next stand till all the stands are visited. Group-3 considers the case that users attend the exhibition in groups such that each member in the group collects contents from specific section or focus of the exhibition. In Group-3, a group has three members and they divide the exhibition into three sections such that each section is assigned to an individual member. Each group member operates in a similar manner as Single-1 but within a section of the exhibition.

We also compare the performance of the algorithm with incentive and service differentiation proposed in [17], MobiFuzzyTrust algorithm proposed by [21] and sybil-resisted trustworthy service evaluation (SrTSE) mechanism in [8]. In service differentiation (ServDiff) mechanism, users in the network are allowed to download contents from their peers just as much as they have shared with others (or contributed to the network). It is a form of tit-for-tat approach where a user is expected to share his contents with his peers and download

contents amounting to the much that he has shared. While this approach has been shown to ensure fairness in the network as users are forced to contribute to the network so that they too can download contents from their peers, this approach does not consider that users may contribute fake or low quality contents to the network to appear to be contributing to the network so as to be able to download contents of interests from the network. MobiFuzzyTrust (MFT) is a semantical trust inference algorithm in MSN that takes into account users' mobile context such as prestige of users, location, time and user's social context so as to evaluate trust between two mobile users. Given the user's context, MFT determines the user's prestige or reputation score, familiarity and similarity scores from the user's social interactions which together with risk of trust are used to compute trust value. MFT incorporates no mechanism of detecting if the user's reviews to be used to infer his reputation are under sybil or rejection attacks discussed earlier in Section V-A. SrTSE is an MSN trust evaluation mechanism where users encrypt their reviews or verify reviews using pseudonym secret keys assigned to them by the local group leader. The group reviews are then aggregated and submitted together to the service provider by the group leader. As group formation or group leader selection in SrTSE is not discussed in [8], we assume that in a time slot, users within $10m$ of the service provider form a group and one user in the group is randomly selected to be the group leader. We assume that a user belongs to only one group in each time slot. Users in a group are assumed to cooperate [8] such that they forward each other's reviews to the group leader without dropping any review. We consider that a malicious group leader can generate pseudonym secret keys and use them to sign multiple reviews and aggregate them into the group's reviews to be submitted to the service provider. We also consider that a malicious group leader can collude with malicious service provider so as to issue him with pseudonym secret keys. This enables the malicious service provider to generate multiple and fake identities so as to self-review his service. Thus, the aggregated group review from the group leader incorporates some random multiple reviews from the group leader while the reviews from the service provider presented to the users contain some random self-reviews from the service provider. So we evaluate the ability of the users to detect these kinds of attacks using SrTSE compared to MCoST. We use (16) to determine trust score of reviews in SrTSE since SrTSE has no formulation to determine trust value. We use *time delay* and *cost* incurred to get contents of interest, and *network utility* together with ability to detect attacks on trust as metrics to evaluate the performance of the proposed scheme.

B. RESULTS

1) MOTIVATING CONTENT SHARING

First, we evaluate the time spent by users to collect their desired contents in the exhibition. As shown in Fig. 9, MCoST reduces user's delay in collecting the contents of interest

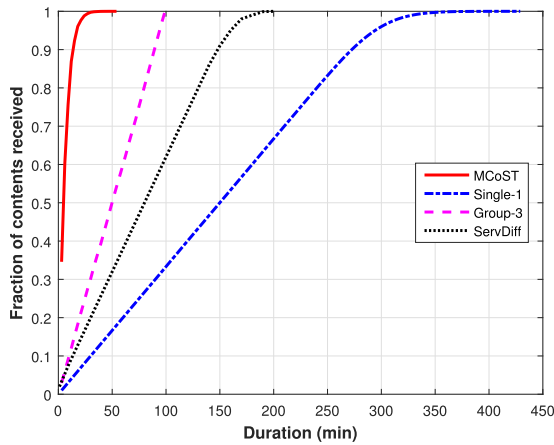


FIGURE 9. Time delay.

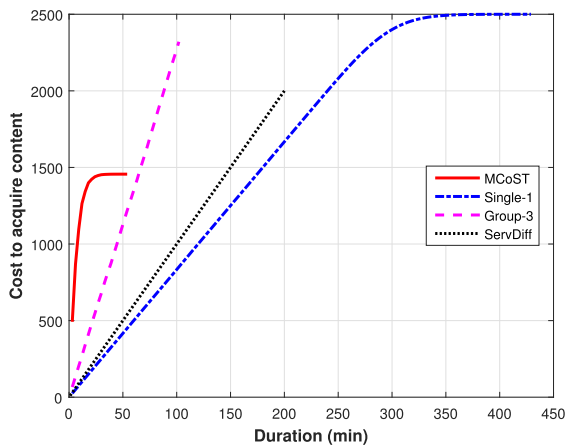


FIGURE 10. Cost.

by 50%, 75% and 86% compared to Group-3, ServDiff and Single-1 respectively. This is because MCoST enables users to collect contents through their encounters and thus they do not have to physically visit all the exhibiting stands to acquire their contents. This way, users get to collect contents of interest in a short time.

Next, we evaluate the cost incurred by users to collect all the contents of interest in the network. This is shown in Fig. 10. We observe that MCoST significantly reduces the cost of content collection. Cost incurred by MCoST is 25%, 35% and 40% lower compared to ServDiff, Group-3 and Single-1 respectively. This is attributed to the collective bidding and cost sharing among the content’s principals incorporated in MCoST. Besides, content’s principals also cut down on the cost that would have been incurred to visit, asses and collect contents from each stand as significant amount of contents are collected through encounters. Lastly, Fig. 11, shows network utilization of the proposed algorithm. Compared to both Single-1, ServDiff and Group-3, MCoST improves network utility by 50%. This is because besides the value and benefit that a user gets in acquiring the desired content, he also receives payments for the content when he shares it. Hence this strategy motivates content sharing while improving network utility.

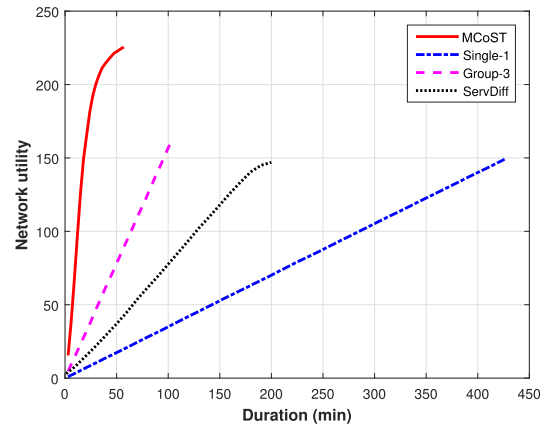


FIGURE 11. Network utility.

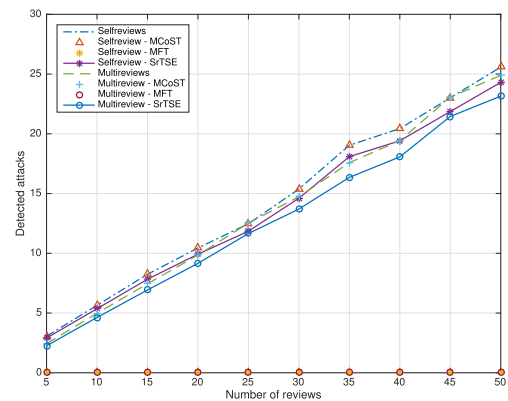


FIGURE 12. Sybil attack detection.

2) CONTENT TRUSTWORTHINESS

First, we consider that review-chain is affected by self-review and multiple review and we wish to establish whether MCoST can detect these attacks. This is shown in Fig. 12. The self-reviews and multi-reviews are plots of self-review and multiple review attacks in the review-chain whereas the other plots indicate the ability of MCoST, SrTSE and MFT to detect these attacks. Notably, MCoST detects all the sybil attacks whereas SrTSE detects some of the attacks and MFT detects none. This is because MCoST ensures that users cannot have multiple and fake identities in the network. In MCoST, a user can only have one public-private key pair generated from the unique registration codes that are assigned to them by the exhibition organizer. In addition, each review record captures the reviewer’s ID, i.e., public key, and thus it is easy to establish if multiple and fake reviews have been submitted by any reviewer in the review-chain. This implies that a review-chain whose reputation and integrity are compromised due to sybil attack cannot disguise as genuine. MFT does not incorporate any mechanism to detect sybil or rejection attacks and thus not able to identify self-reviews, multiple reviews and modifications in a content’s review-chain. While SrTSE ensures that users encrypt their reviews and that a group’s reviews are aggregated and submitted together, it has no mechanism

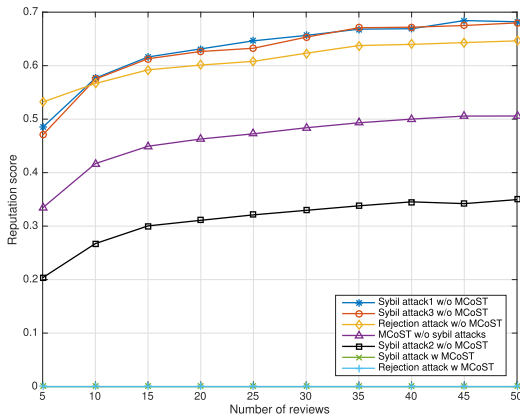


FIGURE 13. Resilience to attacks.

of mitigating or detecting when the group leader becomes malicious and submits multiple and fake reviews as it is the custodian of pseudonym secret keys to be used by the group. Besides, in SrTSE, the service provider can collude with the group leader so as to be issued with the group’s pseudonym secret keys. He can use these keys to generate fake identities and to make self-reviews that may be disguised as genuine reviews. Such attacks are not identifiable by SrTSE which explains its low performance.

Then in Fig. 13, we show the content’s reputation score when its review-chain is under sybil or rejection attack with and without MCoST, and its reputation score if otherwise its review-chain is not under any attack. Without MCoST, sybil attacks 1 and 3, and rejection attack make the content to appear 36%, 35% and 31% more reputable than it actually is while sybil attack 2 reduces the content’s reputation by 33%. This shows the extent to which sybil and rejection attacks can affect the reputation of a content if reviews under these attacks are not detected. With MCoST, the reputation of contents whose reviews are under sybil or rejection attacks are assumed compromised and non-reputable, and thus assigned 0 score. MCoST easily achieves this because it ensures that all reviews in the review-chain are digitally signed by their respective reviewers and that these reviews can accurately be committed to their reviewers. Moreover, in MCoST users share their review history with their peers during their opportunistic encounters which these peers use to validate reliability of review-chains shared by their future encounters. This way, a user can identify rejection attack on a review-chain that he has some of its review history. That is, if any review recorded in the user’s *rh* record to have been made on this encounter’s review-chain about this content is omitted in the review-chain shared by the encounter.

Finally, we show the trust inference using the proposed mechanism considering a content’s review-chain under sybil and rejection attacks and when without these attack. As shown in Fig. 14, using MCoST we can discriminate review-chains under sybil and rejection attacks as their trust

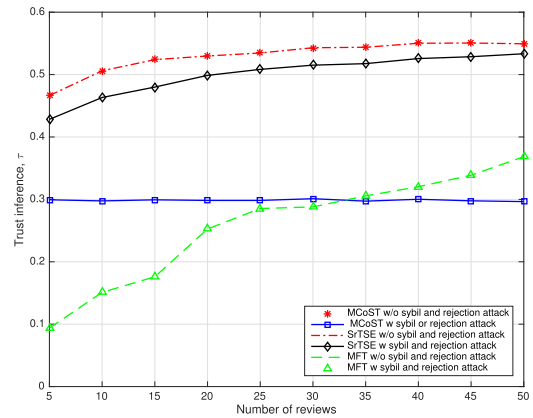


FIGURE 14. Trust inference.

inferences are significantly low. This is because MCoST assigns zero to reputation score of review-chains detected to be under sybil or rejection attack as shown in Fig. 13. Thus, irrespective of the extent to which the content provider is familiar and similar to the user, the similarity and familiarity scores may not be sufficient to elevate the reputation of his content to be perceived as trustworthy by his encounter so long as the content is under sybil or rejection attack. Notably, MFT is built on familiarity, similarity and prestige with no attention to content’s reputation or vulnerability to attacks on content reviews such as sybil or rejection. This makes MFT unable to discriminate reviews under attack. It is observable in Fig. 14 that SrTSE has low ability to discriminate untrustworthy contents from genuine contents. This is because SrTSE is not able to identify self-reviews, and multiple and fake reviews when the group leader becomes malicious or colludes with the service provider. Besides, SrTSE is only able to detect multiple reviews when submitted in the same time slot which deteriorates its performance in opportunistic MSN such as during exhibitions where multiple reviews may be submitted in different time slots. In view of (1), we observe that in setting γ below trust inference of 0.3 in Fig. 14, all contents in the network would be considered trustworthy (including the ones whose review-chains are compromised). However, in setting γ above trust inference of 0.55, some genuine contents whose review-chains are void of sybil and rejection attacks would be considered untrustworthy. This implies that in this case considered, $\gamma \in [0.3, 0.55]$. Thus, setting γ at equidistant of 0.3 and 0.55 would sufficiently discriminate untrustworthy contents whose review-chains are compromised from the genuine contents.

VII. CONCLUSION

We propose a novel mechanism that motivates content sharing and trustworthiness in mobile social network events such as an exhibition. The mechanism is built on collective bidding and cost sharing, and distributed cryptographic hash-chained content reviews that makes it resilient to sybil and rejection attacks. Users propose payments for contents based

on the contents' trustworthiness while content owners share their contents only if the proposed payment can compensate the costs of sharing their contents with users who are interested in them. This guarantees user's individual rationality and thus promotes content sharing in the network and also ensures that the shared contents are trustworthy. Since the reviews are hash-chained, they are undeletable and resistive to modifications as modifying a review in effect changes the review record's hash value and the hash values of all the subsequent review records in the review-chain. This makes such review records invalid as their signed hash values would not match their respective public keys. In addition, users share their review history with their peers during the opportunistic encounters which these peers use to establish the integrity of review-chains shared by their future encounters. Simulation results show that the proposed mechanism reduces the time and cost to collect the contents of interest in the network and significantly improves network utilization. Moreover, it efficiently evaluates content's trustworthiness by detecting and discriminating review-chains whose reputation are compromised due to sybil or rejection attack.

REFERENCES

- [1] A. Beach et al., "WhoThat? Evolving an ecosystem for context-aware mobile social networks," *IEEE Netw.*, vol. 22, no. 4, pp. 50–55, Jul. 2008.
- [2] Z. Mao, Y. Jiang, G. Min, S. Leng, X. Jin, and K. Yang, "Mobile social networks: Design requirements, architecture, and state-of-the-art technology," *Comput. Commun.*, vol. 100, pp. 1–19, Mar. 2017.
- [3] C. C. Aggarwal, Ed., "An introduction to social network data analytics," in *Social Network Data Analytics*. New York, NY, USA: Springer, 2011, pp. 1–15.
- [4] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2435–2443.
- [5] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1647–1655.
- [6] Y. Najafloo, B. Jedari, F. Xia, L. T. Yang, and M. S. Obaidat, "Safety challenges and solutions in mobile social networks," *IEEE Syst. J.*, vol. 9, no. 3, pp. 834–854, Sep. 2013.
- [7] C. Wu, T. Luo, F. Wu, and G. Chen, "Endortrust: An endorsement-based reputation system for trustworthy and heterogeneous crowdsourcing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
- [8] X. Liang, X. Lin, and X. S. Shen, "Enabling trustworthy service evaluation in service-oriented mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 310–320, Feb. 2014.
- [9] D. Quercia and S. Hailes, "Sybil attacks against mobile users: Friends and foes to the rescue," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–5.
- [10] T. Ning, Y. Liu, Z. Yang, and H. Wu, "Incentive mechanisms for data dissemination in autonomous mobile social networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3084–3099, Nov. 2017.
- [11] K. C.-J. Lin, C.-W. Chen, and C.-F. Chou, "Preference-aware content dissemination in opportunistic mobile social networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1960–1968.
- [12] X. Kang and Y. Wu, "Incentive mechanism design for heterogeneous peer-to-peer networks: A Stackelberg game approach," *IEEE Trans. Mobile Comput.*, vol. 14, no. 5, pp. 1018–1030, May 2015.
- [13] F. M. Awuor, C.-Y. Wang, and T.-C. Tsai, "Motivating content sharing in mobile social network through collective bidding," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018.
- [14] T. Ning, Z. Yang, H. Wu, and Z. Han, "Self-interest-driven incentives for ad dissemination in autonomous mobile social networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2310–2318.
- [15] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6692–6702, Aug. 2016.
- [16] J. Park and M. van der Schaar, "A game theoretic analysis of incentives in content production and sharing over peer-to-peer networks," *IEEE J. Sel. Topics Signal Process.*, vol. 4, no. 4, pp. 704–717, Aug. 2010.
- [17] R. T. B. Ma, S. C. M. Lee, J. C. S. Lui, and D. K. Y. Yau, "A game theoretic approach to provide incentive and service differentiation in P2P networks," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 32, no. 1, pp. 189–198, 2004.
- [18] X. Zhang, Z. Yang, Z. Zhou, H. Cai, L. Chen, and X. Li, "Free market of crowdsourcing: Incentive mechanism design for mobile sensing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3190–3200, Dec. 2014.
- [19] T. Luo, H.-P. Tan, and L. Xia, "Profit-maximizing incentive for participatory sensing," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Apr./May 2014, pp. 127–135.
- [20] S. Trifunovic, F. Legendre, and C. Anastasiades, "Social trust in opportunistic networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM)*, Mar. 2010, pp. 1–6.
- [21] F. Hao, G. Min, M. Lin, C. Luo, and L. T. Yang, "Mobifuzzytrust: An efficient fuzzy trust inference mechanism in mobile social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 11, pp. 2944–2955, Nov. 2014.
- [22] K. Bicakci and N. Baykal, "Infinite length hash chains and their applications," in *Proc. 11th IEEE Int. Workshops Enabling Technol., Infrastruct. Collaborative Enterprises (WET ICE)*, Jun. 2002, pp. 57–61.
- [23] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, 2006, pp. 420–436.
- [24] G. Sheng, C. Tang, H. Han, W. Gao, and X. Hu, "Authentication of outsourced linear function query with efficient updates," *Cluster Comput.*, vol. 9, pp. 1–9, Jul. 2017.
- [25] H. Pang and K. Mouratidis, "Authenticating the query results of text search engines," *Proc. VLDB Endow.*, vol. 1, no. 1, pp. 126–137, Aug. 2008. [Online]. Available: <http://dx.doi.org/10.14778/1453856.1453875>
- [26] S. Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: 2008. [online] Available: <http://bitcoin.org/bitcoin.pdf>
- [27] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.
- [28] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain—The gateway to trust-free cryptographic transactions," in *Proc. 24th Eur. Conf. Inf. Syst. (ECIS)*, 2016, p. 153.
- [29] A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*. Sebastopol, CA, USA: O'Reilly Media, 2017.
- [30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies—A Comprehensive Introduction*. Princeton, NJ, USA: Princeton Univ. Press, 2016.
- [31] A. Chin and D. Zhang, Eds., *Mobile Social Networking: An Innovative Approach*. New York, NY, USA: Springer, Springer-Verlag, 2014.
- [32] W. Jiang, G. Wang, M. Z. A. Bhuiyan, and J. Wu, "Understanding graph-based trust evaluation in online social networks: Methodologies and challenges," *ACM Comput. Surv.*, vol. 49, no. 1, p. 10, 2016.
- [33] A. Josang and R. Ismail, "The beta reputation system," in *Proc. 15th Bled Electron. Commerce Conf.*, vol. 5, 2002, pp. 2502–2511.
- [34] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket switched networks and human mobility in conference environments," in *Proc. ACM SIGCOMM Workshop Delay-Tolerant Netw.*, 2005, pp. 244–251.
- [35] A.-K. Pietiläinen and C. Diot, "Dissemination in opportunistic social networks: The role of temporal communities," in *Proc. 13th ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2012, pp. 165–174.
- [36] A. Chaintreau, A. Mtibaa, L. Massoulie, and C. Diot, "The diameter of opportunistic mobile networks," in *Proc. ACM CoNEXT Conf.*, 2007, p. 12.
- [37] R. Lan, W. Wang, A. Huang, and H. Shan, "Device-to-device offloading with proactive caching in mobile cellular networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
- [38] W. Sherchan, S. Nepal, and C. Paris, "A survey of trust in social networks," *ACM Comput. Surv.*, vol. 45, no. 4, 2013, Art. no. 47.
- [39] D. Crandall, D. Cosley, D. Huttenlocher, J. Kleinberg, and S. Suri, "Feedback effects between similarity and social influence in online communities," in *Proc. 14th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, 2008, pp. 160–168.



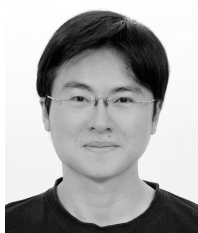
FREDRICK MZEE AWUOR received the B.S. degree in computer science from Moi University, Eldoret, Kenya, in 2008, and the M.Tech. degree in electrical engineering from the Tshwane University of Technology, Pretoria, South Africa, in 2012. He is currently pursuing the Ph.D. degree in social networks and human centered computing from National Chengchi University in collaboration with Academia Sinica, Taipei, Taiwan. His research interests include

social networks, wireless communication, and network economics.



TZU-CHIEH TSAI was born in Tainan, Taiwan. He received the B.S. degree in electrical engineering from National Taiwan University in 1988, the M.S. degree in electrical engineering from the University of Southern California in 1991, and the Ph.D. degree in computer science from the University of California at Los Angeles (UCLA) in 1996. After that, he joined UCLA in 1991. From 2005 to 2008, he was the Chair of the Department of Computer Science, National Chengchi University, Taipei, Taiwan, where he is currently an Associate Professor.

...



CHIH-YU WANG received the B.S. and Ph.D. degrees in electrical engineering and communication engineering from National Taiwan University, Taipei, Taiwan, in 2007 and 2013, respectively. He was a Visiting Student with the University of Maryland at College Park, College Park, in 2011. He is currently an Assistant Research Fellow with the Research Center for Information Technology Innovation, Academia Sinica, Taipei. His research interests include game

theory, wireless communications, social networks, and data science.