Peer Collaboration in Wireless Ad Hoc Networks

Lin Cai[1], Jianping Pan[2], Xuemin (Sherman) Shen[1], and Jon W. Mark[1]

[1] University of Waterloo, Waterloo, Ontario N2L 3G1, Canada
[2] NTT MCL, Palo Alto, California 94306, USA

Abstract. Voluntary peer collaboration is often assumed in media access, route discovery, packet forwarding, and upper-layer protocols for wireless ad hoc networks. This assumption is seriously challenged when some peers are autonomous, selfish, or malicious in large-scale, heterogeneous networks. In this paper, based on the latest advances in identity-based cryptography, we design a lightweight and cheat-resistant micropayment scheme to stimulate and compensate collaborative peers that sacrifice their resources to relay packets for other peers. We also demonstrate that when security and collaboration measures are properly enforced, profitable collaboration is a preferable strategy for all peers.

1 Introduction

Wireless ad hoc networks are self-organized systems without relying on any pre-existing, fixed communication infrastructures, so individual peers have to assist communications that are vital for other peers. Wireless ad hoc networks are especially attractive when infrastructures are too expensive to build, or too vulnerable to maintain [1,2], and have attracted much attention in recent years [3,4]. *Voluntary collaboration* is often assumed among involved peers, which is acceptable when all peers are genuine, collaborative, and under the control of a single authority. As indicated in [5–12], the validity of this assumption is challenged when some peers are autonomous, selfish, or malicious. For example, if battery-powered peers relay packets for other peers, they are one-step closer to running out of their energy, which is undesirable from a selfish standpoint, since they may have insufficient energy to send their own packets later.

In this paper, we are interested in secure collaboration of *selfish* peers in energy-constrained wireless ad hoc networks. In our setting, a peer (e.g. a user carrying a battery-powered laptop computer with wireless LAN interfaces) joins a group of other peers. These peers may or may not have preestablished trustworthiness (e.g. in a public recreation park), or share any common goals (e.g. accessing the Internet or swapping files). A peer may raise the output power of its transmitter to communicate with intended peers directly; however, its capability to do so in practice is always limited by hardware design, and such a strategy may not be preferred by other peers (due to higher interference) or even by itself (due to higher energy consumption). Hence, collaborations among neighboring peers (e.g. relaying) are essential in wireless ad hoc networks.
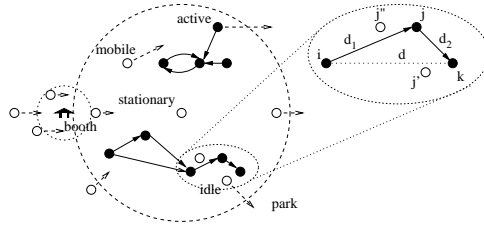
Fig. 1. Relaying in wireless ad hoc networks.

The desire to collaborate in wireless ad hoc networks faces many new challenges. First, peers have to be assured that they indeed exchange information with intended peers, even when they no longer communicate with each other directly. Second, as packets are relayed by peers without preestablished trustworthiness, peers have to be assured that the confidentiality, integrity, and authenticity of exchanged information are not compromised. Third, selfish peers always want to take advantage of other peers, but hesitate to help others if their resources are sacrificed, so certain measures are required to stimulate and compensate favorable collaborations. Finally, the entire system should benefit from secure collaboration among selfish peers, and resist against malfunctioning or malicious peers; otherwise, peers tend to remain selfish.

In contrast to many existing approaches (see Sect. 5 for related work), we apply the latest advances in identity-based cryptography (IBC) [13] to ad hoc networks. IBC is a form of public-key cryptography (PKC). Unlike regular PKC systems, in which the binding between the identity of an entity and its public-key should be certified by certificate authorities (CAs) or stored in central directories, such authorities and directories can be completely eliminated in IBC systems, in which the public-key of an entity can be derived from its identity directly. This property is vitally important for wireless ad hoc networks, where public-key infrastructures (PKIs) or CA hierarchies are generally expensive to build and maintain. IBC is used to facilitate asymmetric encryption/decryption and signature/verification procedures; it can also be used to bootstrap their symmetric counterparts without prearranging pairwise shared secrets among all involved peers. Based on IBC, a lightweight and cheat-resistant micropayment scheme can be devised for ad hoc networks, which stimulates and compensates collaborative peers that sacrifice their resources to help others.

The remainder of this paper is organized as follows. In Sect. 2, we present the model for ad hoc networks, their security requirements, and our IBC-based approaches. In Sect. 3, we design an IBC-based micropayment scheme to stimulate and compensate collaborative peers. Through the performance studies in Sect. 4, we show that profitable collaboration is preferable if properly enforced. Sect. 5 reviews related work, and Sect. 6 concludes this paper.

2 Secure Communications

Network model — As shown in Fig. 1, wireless ad hoc networks are fully-distributed systems of self-organizing peers that wish to exchange information

over-the-air but do not rely on any preexisting infrastructures [1–4]. Mobile peers (e.g. laptop computers, shown as dots, with wireless interfaces) can join or leave such systems (depicted by a large dashed circle, e.g. a recreation park) at any time. Only peers require keying have to pass by an offline authority regularly (e.g. a ticketing booth within a small dotted circle). Without any centralized online authorities, peers can remain stationary or mobile, keep idle (unfilled dots) or active (filled dots), and assist others if they choose to do so.

Let peer i in Fig. 1 transmit a bulk of data b to another peer k that is d away. i can have two options: 1) i transmits b to k directly, and consumes energy $e_i^t(b, d) = (t_1 + t_2 d^{n(d)})b$, where $2 \leq n(d) \leq 6$ is the path loss exponent, and t_1 and t_2 are the coefficients of distance-independent and related energy consumption. i cannot always do so if $d > D$ and D is its maximum transmission range. 2) When there is a third peer j between i and k, i may save energy by requesting j to relay b to k. Without loss of generality, assume j is d_1 away from i, and d_2 from k. If $d_1 < d$, relaying b through j is preferable for i, while j has to volunteer $e_j^r(b) = r_1 b$ to receive b from i, $e_j^t(b, d_2) = (t_1 + t_2 d_2^{n(d)})b$ to transmit b to k, and $e_j^o(b)$ to cover local expenses. If $e_i^t(b, d) - e_i^t(b, d_1) > e_j^r(b) + e_j^t(b, d_2) + e_j^o(b)$, relaying through j is also preferable for the entire system, since overall it takes less energy to move the same b from i to k. When all peers are voluntary and relaying is favorable, relaying should be mandated. But if j is autonomous, it has no incentive to relay b from i to k; if j is selfish, it will refuse to relay b, since j has to sacrifice its own resources for the benefit of others.

If k is the beneficiary of transferring b directly from i, k should be willing to pay i at least $c_i(b, d) + c_i(b)$ to cover the communication expense occurred at i and the cost for i to obtain b. $c_i(b, d)$ is proportional to $e_i^t(b, d)$ and may be reversely proportional to the remaining energy ϵ_i of i. When relaying is favorable, k finds that it is more cost-effective to retrieve b from j, after j has obtained b from i. To do so, j has to pay i at least $c_j(b) = c_i(b, d_1) + c_i(b)$, and k has to pay j at least $c_j(b, d_2) + c_j(b)$ in advance. If $c_i(b, d) > c_i(b, d_1) + c_j(b, d_2)$, k has enough cost-saving to share with j. For simplicity, we assume j and k share the cost-saving equally; i.e., the net cost-saving at k is $[c_i(b, d) - c_i(b, d_1) - c_j(b, d_2)]/2$, which is also the profit j can make through its relaying.

Security model — Many security threats appear in wireless ad hoc networks [14]. Peers can join or leave at any time without notice, and pairwise trustworthiness among all peers is impractical to build and unrealistic to maintain. Autonomous peers have reasons and excuses to eavesdrop or corrupt relayed data. Malicious peers can impersonate other peers to steal genuine information or inject false information. When relaying is profitable, selfish peers have strong incentives to boost their wealth improperly, by cheating source, destination, or other relaying peers. When there is a certain number of colluding peers, they may even attempt to fool or beat the entire system.

Traditional cryptographic techniques are employed to provide certain security properties in networks with trusted infrastructures. Similar efforts have been attempted in wireless networks: source and destination peers should authenticate to each other before information exchange; also, information should be encrypted

by sources to keep confidentiality, and be verified by destinations to preserve integrity. These procedures rely on either certified public-keys in PKC systems, or pairwise prearranged secrets in symmetric cryptography systems. If there are trusted infrastructures (e.g. genuine PKIs or base-stations in cellular systems), such prerequisites can be satisfied accordingly.

However, these techniques do not readily apply to wireless ad hoc networks. First, there are no genuine PKIs or online authorities that can always be involved in communications among any peers. Second, most end-to-end communications in ad hoc networks occur in a hop-by-hop manner, where untrusted third-parties are required to relay packets, so security proprieties should be achieved not only at the end-to-end level, but also at the per-hop level. For example, in Fig. 1, j pays i to obtain b for k; but j's neighbor j' can overhear the communication between i and j, and offers b to k at a lower price. Finally, most existing electronic payment schemes either rely on online, interactive authorities (e.g. banks), or are too heavy (in terms of computation and communication complexity) for wireless ad hoc networks, where energy constraints are the foremost concern.

IBC-based approaches — The concept of IBC was first introduced by Shamir two decades ago [15]. The first efficient and secure IBE scheme (BF-IBE) was given in 2001 by Boneh and Franklin, which employs Weil pairing on elliptic curves [16]; its security is based on the bilinear Diffie-Hellman problem (BDHP), which is considered secure in the random oracle model (ROM).

In IBC-based wireless ad hoc networks, each peer proposes its identity (e.g. *a@b.com*, service name, content hash, etc.), which is also its public-key [17]. A private-key generator (PKG, e.g. the ticketing booth in recreation park) verifies identity ownership, appends timestamp for unique identities, and extracts a corresponding private-key from the public system parameters and the master-key only known to PKGs. To reduce the risk of total-exposure with compromised PKGs, and to ease the concern of key escrow with bogus PKGs, the master-key can be distributed in a t-of-n manner to n PKGs with threshold cryptography [18]. Also, hierarchical PKGs allow communications with roaming peers to be protected by their identity and the system parameters of root PKG [19].

When a peer i sends a message m to another peer k, m is encrypted with k's identity id_k and the system parameters; only k can decrypt the encrypted $\hat{m}$ with its private-key pk_k and the system parameters. When k acknowledges m, the receipt is signed with pk_k, and is verifiable by everyone knowing id_k. i knows id_k when communicating with k, and no one else can compromise these procedures without knowing pk_k. IBC also supports authenticated and signed encryption. In addition, IBC can establish a shared-key $sk_{i,k}$ for i and k from their identity id_i and id_k. Using bootstrapped shared-keys, instead of pairwise prearranged secrets, peers can utilize symmetric and more efficient encryption/decryption and message authentication schemes (e.g. HMAC).

Our next step is to stimulate selfish peers to collaborate (i.e. relaying for others), and compensate them if they do so. Here, we focus on a receiver-payer model; other payment models (e.g. sender-payer) can be accommodated by pre-fixing application-layer payments to our scheme.
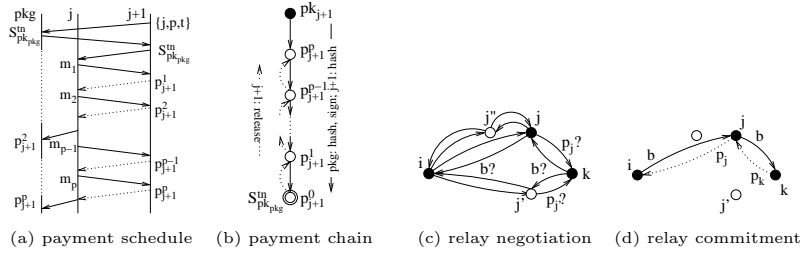
(a) payment schedule   (b) payment chain   (c) relay negotiation   (d) relay commitment

Fig. 2. Per-hop and end-to-end transactions.

3   Collaborative Communications

Hop-by-hop transactions — We first focus on the data transfer and payment scheme between two adjacent peers, j and $j + 1$. Assume $j + 1$ is willing to pay at least $p = c_j(b) + c_j(b, d)$ to obtain b from j, and j agrees. As shown in Fig. 2(a), to facilitate this transaction with sequence number tn, $j + 1$ securely contacts a non-interactive entity (for simplicity, we assume the PKG plays this role) to commit deposited credits of amount p to this transaction. For notational convenience, we assume j, $j+1$, and the PKG have bootstrapped pairwise shared-keys from their identity. The commitment proposal message sent by $j + 1$ is $CPPS\{id_{pkg}, tn, id_{j+1}, id_j, p, et\}_{sk_{pkg,j+1}}$, where et indicates the expiry time. As shown in Fig. 2(b), the PKG hashes $j + 1$'s private-key pk_{j+1} with j's identity id_j repeatedly for $p+1$ times, i.e. $p_{j+1}^{p-1} = H_{id_j}(tn||p_{j+1}^p||et)$, and signs p_{j+1}^0 with its own private-key pk_{pkg}, i.e. $S_{pk_{pkg}}^{tn} = S_{pk_{pkg}}(tn||p_{j+1}^0||et)$, where $S_{pk}(\cdot)$ is the signing procedure with key pk. Only $S_{pk_{pkg}}^{tn}$, instead of the entire hash-chain, is required to be sent back to $j + 1$ securely; only p_{j+1}^0 is kept by the PKG as a record of this transaction. The commitment confirmation message sent by the PKG to $j + 1$ is $CCFM\{id_{j+1}, tn, id_{pkg}, id_j, S_{pk_{pkg}}^{tn}, et\}_{sk_{pkg,j+1}}$.

$j + 1$ rebuilds the hash-chain from its private-key pk_{j+1}, and securely reveals $S_{pk_{pkg}}^{tn}$ to j in $HCMT\{id_j, tn, id_{j+1}, S_{pk_{pkg}}^{tn}, et\}_{sk_{j,j+1}}$. The authenticity of $S_{pk_{pkg}}^{tn}$ can be easily verified by j alone with the PKG's identity id_{pkg}. Once j starts to transmit message m_i of b to $j + 1$ in $HMSG\{id_{j+1}, tn, id_j, m_i, et\}_{sk_{j,j+1}}$, and after the authenticity of m_i is verified, $j + 1$ releases the hash-chain gradually in a reverse order (i.e. p_1, p_2, $\cdots$, p^p) in $HPMT\{id_j, tn, id_{j+1}, p_{j+1}^i, et\}_{sk_{j,j+1}}$. j can verify the authenticity of p_{j+1}^i alone by keeping a copy of p_{j+1}^{i-1}, the last payment from $j+1$, since $p_{j+1}^{i-1} = H_{id_j}(tn||p_{j+1}^i||et)$. The discrepancy of the data transfer and payment between j and $j + 1$ is at most one unit. j only keeps the latest (instead of every) payment from $j + 1$ as its record.

At any time, j can submit the latest payment from $j + 1$ to the PKG in $HCLM\{id_{pkg}, tn, id_j, id_{j+1}, p_{j+1}^i, et\}_{sk_{pkg,j}}$ to claim the actual compensation. The PKG only keeps the latest record submitted by j of the hash-chain committed by $j + 1$ as its record. j has to inverse a one-way hash function to claim the payment not received yet (i.e. false claim), which is not feasible.

In our design, $j+1$ cannot deny released payments after it receives m_i from j (except at most one unit discrepancy), since if j has p_{j+1}^i, the PKG knows $j + 1$

should have paid j for i times of unit amount. If $j+1$ overspends the hash-chain, it has to reveal its private-key to j, which leads to a more serious consequence for $j + 1$ (e.g. j can impersonate $j + 1$ to claim $j + 1$'s remaining balances). $j+1$ cannot double-spend a single payment without being detected by j, since j always verifies the latest payment by hashing. Also, $j + 1$ cannot double-spend a single hash-chain containing j's identity for transactions with other peers, since they always verify the authenticity of received payments with their own identity. Even if colluding peers forge nonexistent relaying and payments, their overall wealth does not increase. Therefore, selfish peers have no incentives to collude with other peers and risk their own privacy and wealth.

Furthermore, neither j nor $j + 1$ has to contact the non-interactive PKG during a transaction, unless j or $j+1$ aborts the transaction or j wants to claim payments in batch. With the kept p_{j+1}^0, the PKG can easily find the proper amount j should claim by hashing p_{j+1}^i repeatedly alone. If j indicates the end of the transaction (as a courtesy to $j+1$), the balance of this hash-chain, if any, is refunded to $j + 1$ immediately (i.e. instant refund), which can be achieved by the PKG hashing $j + 1$'s private-key with j's identity repeatedly alone again. If j does not indicate so, the balance will be refunded to $j + 1$ by the PKG automatically when the hash-chain expires (expiry refund), which is indicated in $S_{pk_{pkg}}^{tn}$, so j has to claim received payments before expiry.

End-to-end transactions — As shown in Fig. 2(c), when a peer k wants to obtain b, it broadcasts an authenticated solicitation with sequence number sn to its neighbors for the availability of b and the cost of obtaining b in $SLCT\{id_i, sn, id_k, if(b)\}_{pk_k}$, where i is a potential source of b and $if(b)$ is the meta-information about b. A neighboring peer, e.g. j, can repeat the same solicitation authenticated on its own behalf, if it anticipates its relaying profitable. Within a time window, a peer does not respond to a solicitation that is a subset of its own. In Fig. 2(c), two other peers, j' and j'', follow the same procedure as j does. The solicitation repeats recursively and finally arrives at a peer, e.g. i, that has b available and is willing to offer b to j, j', and j''.

Assume j receives offers from i and j'' securely, and finds it costs less to retrieve b from i directly. Based on its profit strategy, j offers b to k at a price p_j in $RSPS\{\{id_i, sn, id_k, if(b)\}_{pk_k}, id_j, p_j\}_{sk_{j,k}}$, which is profitable for j and supposedly acceptable for k. j has to offer b at a competitive price, since there are other peers competing with j; otherwise, k prefers to deal with others at a better price, and j loses the potential profit from k completely.

Within a time window after its solicitation, k decides whether to obtain b from one of its relaying candidates at a price favorable to itself, or just gives up when none of the received offers is affordable. If the first case happens, k follows the designed per-hop transactions with the chosen relaying peer, so do the upstream relaying peers, as shown in Fig. 2(d). Source peer i should prepare b in a proper format for relaying, e.g. $\{\{m_1\}_{pk_i}, \{m_2\}_{pk_i}, \cdots, \{m_n\}_{pk_i}\}$, where $\{\cdot\}_{pk_i}$ implies these messages are protected in an end-to-end manner by i's signature, so downstream peers can verify the relayed messages and compensate upstream peers independently. If i knows all involved downstream peers (e.g. j and k)

with a static route, i can apply an onion-like HMAC chain to each message with the shared-key bootstrapped from their identity, i.e. $\{\{\{m_i\}_{sk_{i,k}}\}_{sk_{i,j}}\}$, which can be verified by j using its shared-key with i. j then passes $\{\{m_i\}_{sk_{i,k}}\}$ to k, which can be verified by k. If the second case happens, k can either increase its broadcast radius (in case k has a hostile neighborhood), move to a location closer to i, or solicit b later when b is cached at nearby peers.

When k obtains b relayed by j from i, it has to pay two types of expense: the cost associated with b (e.g. the cost for i to obtain b, or the value of b assigned by its creator), and the cost to move b from i to k. Here, we decompose end-to-end transactions between the source and destination peer of b into a series of per-hop transactions, so peers only deal with their neighboring peers. Essentially, neighboring peers send upstream peers payments to receive b, and meanwhile receive payments from downstream peers to send b. Since relaying may reduce the overall cost for k to obtain b, k should be willing to share the cost-saving with relaying peers. This *profitability principle* stimulates profitable collaborations among selfish peers in wireless ad hoc networks.

Collaboration strategies — With our security and collaboration measures, peers can have three basic strategies. First, a *voluntary* peer relays for all other peers. Second, a peer is selfish in general, but it becomes *collaborative* only if it is profitably compensated, either by the explicit payment from requesting peers, or by the extracted value of relayed data. Third, a *solely selfish* peer does not relay for others, i.e. it is always non-collaborative.

There are many alternatives to these strategies. For instance, a peer can selectively collaborate with peers that have been collaborative to itself. Also, a peer can choose to follow different strategies throughout its lifetime in the system: initially, it is voluntary when it has plenty of energy; later, it becomes energy-conscious and collaborative only if it is profitably compensated; when its on-board energy is low, it becomes solely selfish and does not relay for others at all. For presentation simplicity, we only consider peers with a chosen strategy throughout their lifetime in a system with different mixes of voluntary, collaborative, and selfish peers in our numerical study.

4   Performance Evaluation

Evaluation approach — We consider a wireless ad hoc network with the topology shown in Fig. 3(a), where N peers are randomly located on a ring of radius R. With an intentionally-rounded topology, peers have no location disadvantages when compared with peers at any other locations (in contrast, peers close to the border of a finite topology tend to have greater distances to most other peers). This approach allows us to *exclusively* investigate the performance impact of collaboration strategies in wireless ad hoc networks. Arbitrary topologies can be compensated by peer density, preferable pricing, and other means.

When a peer with a certain amount of energy joins the network, it obtains its private-key from the PKG, and deposits a certain amount of monetary credits at the PKG to compensate relaying peers (and the PKG for control traffic).
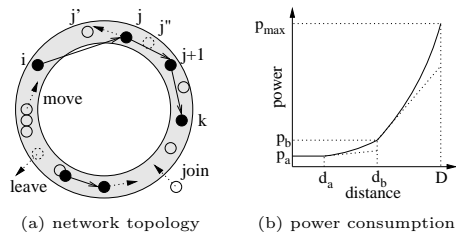
(a) network topology (b) power consumption

Fig. 3. Simulation configurations.

Fig. 4. Peer demography

#	peer %			demographic
	V	CiC	SS	scenario
I	100	0	0	all voluntary
II	0	0	100	all selfish
III	30	40	30	a general case
IV	0	100	0	all collaborative

Periodically, peers can trade their accumulated credits for on-board energy (e.g. batteries), and vice versa. The total wealth of a peer is measured by the amount of its remaining energy, available credits, and the value of obtained information. When a peer runs out of energy and credits, it is presumably dead.

Peers can be voluntary (V), collaborative if compensated (CiC), or solely selfish (SS). Their communication cost relies on the distance over which the transferred data cross. As shown in Fig. 3(b), when distance d is less than a threshold d_a, the transmission power consumption remains constant, i.e. $n(d) = 0$ when $0 < d \leq d_a$, and relaying does not offer additional cost-saving. Once $d > d_a$, the distance-related transmission power consumption becomes dominant. When $d_a < d \leq d_b$, relaying is preferable but not critical, e.g. $n(d) = 2$; when $d > d_b$, relaying becomes very attractive by offering significant cost-saving, e.g. $n(d) \geq 4$. The maximum output power ($p_{\max}$) of its transmitter limits the distance that a peer can reach, so $d \leq D$. Here, we set $D < 2R$ intentionally, and peers cannot always communicate with their intended peers directly.

Numerical results — The results presented here are for an IBC-powered wireless ad hoc network of $N = 64$ and $R = 10$. For comparison purpose, all V, CiC, and SS peers have the same amount of initial energy and credits, and are randomly located on the ring. A peer requests data of size 1 to 100 unit length from other peers randomly. We consider four 4 scenarios listed in Tab. 4.

The per-peer performance metrics considered are: the sum of remaining energy and available credits; the volume of obtained information; the volume of missed information due to insufficient energy and credits. From the standpoint of an individual peer, it expects more remaining energy and available credits, more obtained information, and less missed information. For the whole system, the performance metric is the amount of data transferred per unit energy and per unit distance, which reflects the utility of the system employing these measures to facilitate collaboration among peers. We intentionally create an energy-challenged situation by allowing peers to actively request data from other peers (1 request per 100 time unit on average with Poisson distribution), so peers are very likely to miss information due to insufficient energy and/or credits. The *value* of obtained information is weighed by the distance over which the data cross, i.e. if a peer wants to obtain data from a remote peer, it implies that the information is of more value than that from a nearby peer.

In Fig. 5(a), we plot average remaining energy and available credits, normalized to the initial ones, of peers in different demographic scenarios. To avoid warming-up effects, we collect system logs 100 unit time after initialization. Also,

(a) different demographic scenarios

(b) general demographic scenario

(c) obtained information value

(d) missed information ratio
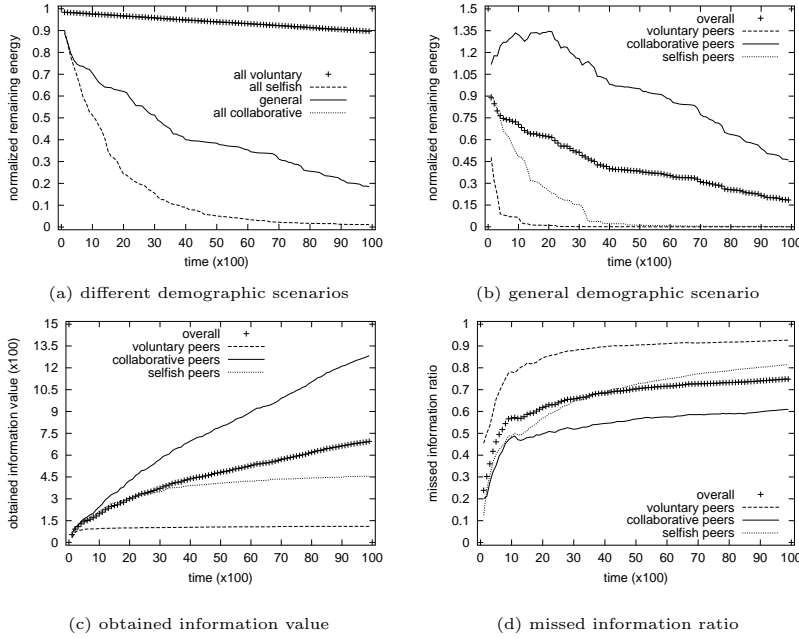
Fig. 5. Numerical results for per-peer performance metrics.

results are averaged for 100 runs. When all peers are voluntary (scenario I), a peer always relays packets for others. This is the case when the system is running in the optimal region. On the contrary, when all peers are selfish (scenario II), no peer relays for others, and vice versa; they eventually consume more energy (i.e. a quick drop in remaining energy) to directly communicate with intended peers when feasible, and miss more information when infeasible. When there are certain collaborative peers (about 40% in scenario III), profitable relaying is preferred by these peers, and the overall average remaining energy is considerably higher than that in scenario II. When all peers are collaborative if properly compensated (scenario IV), a significant amount of energy is conserved, and the system is running in a region close to the optimal one in scenario I.

Fig. 5(b) decomposes the normalized remaining energy for V, CiC, and SS peers in the general demographic scenario (i.e. scenario III). V peers always relay for others, no matter compensated or not; they will attract a lot of selfish peers, and their on-board energy is quickly dissipated. As seen in this figure, V peers almost run out of energy within the first quarter of simulation, due to heavy relaying requests from their neighbors. SS peers take advantage of their neighboring V peers aggressively, so initially their remaining energy reduces relatively slowly when there are many V peers around. When V peers are out of energy, SS peers no longer have free ride. Even worse, since V peers are more likely out of energy when they have SS neighbors, these SS peers eventually pay higher cost to transfer data over greater distances. CiC peers, on the other hand, accumulate credits when they relay for others, and purchase energy when necessary; they conserve energy much better than V and SS peers.

Table 1. System performance metrics

scenario		consumed energy (%)	obtained information	average utility
	overall	81.5	694.508	852.157
III	V	100.0	110.550	110.550
	CiC	53.9	1283.308	2380.905
	S	99.7	455.619	456.990

In Fig. 5(c), we show the obtained information value for V, CiC, and SS peers in scenario III. Due to their capability to make profit by relaying packets for others and to conserve remaining energy, CiC peers obtain much more information than V and SS peers. Combining Fig. 5(b) and Fig. 5(c), it is easy to see peer collaboration increases system utility with more obtained information and less consumed energy. This observation is confirmed by the numbers listed in Tab. 1. On average, a unit of energy can transfer about 852.157 unit of data across unit distance for all peers in the system. V peers have the lowest utility of 110.157. Although S peers have a higher utility of 456.990 than V peers by taking advantage of nearby V peers, it is still very surprising to see that S peers indeed have a much lower utility than CiC peers.

Fig. 5(d) gives the ratio of missed information value among all requested information. As we mentioned, we stretch the capability of collaboration schemes in a severely energy-challenged situation, and peers are very likely to miss information. However, as we can see in this figure, CiC peers still outperform V and SS peers. For V peers, their energy is more likely consumed by relaying for others, so they suffer the highest miss ratio. SS peers take advantage of V peers, and have similar performance with CiC peers initially when there are many V peers around. Once most V peers are out of energy, SS peers suffer a much higher information miss ratio as well.

Through these studies, it is concluded that when security and collaboration measures are properly enforced, profitable collaboration is a preferable strategy for all peers in wireless ad hoc networks. Also, with profitable collaboration, system utility increases when peers have maximized their potential profit, which motivates wireless ad hoc networks to adopt these measures.

5 Related Work

Wireless ad hoc networks have attracted intensive attention in recent years [1–4]. Their intrinsic vulnerabilities due to the lack of communication and security infrastructures, secured media, trusted peers, and stable states have geared a considerable amount of research efforts toward securing information exchange in these systems [14, 18, 20–25]. Also, the assumption of voluntary collaboration in wireless ad hoc networks begins to be challenged.

Watchdog and pathrater with overhearing are proposed in [5] to identify peers that agree but fail to forward packets. A majority voting scheme is proposed in [6] to identify misbehaviors by consensus. Packet purse model (PPM) and packet trade model (PTM) [7] use tamper-resistant hardware to circulate and exchange nuglets (a virtual currency). A reputation-based scheme is proposed in [8] to identify and isolate misbehaving peers. CORE also employs watchdog, but has

a more sophisticated reputation system to differentiate subjective, indirect, and functional reputation [9]. In Sprite [11], relaying peers keep hashed receipts of forwarded messages, and later claim credits from a central authority when a fast connection is available. Besides fully-distributed wireless ad hoc networks, peer collaboration is also studied in multi-hop cellular systems, where base-stations are available to facilitate and reward collaborative peers. A lottery-like scheme is proposed in [10], where a payee only needs to claim a few winning tickets [26]. A charging and rewarding scheme [12] takes advantage of a trusted base-station that is always involved in communications between any two peers.

In contrast, our hash-chain-based micropayment scheme focuses on *profitable* collaboration among *selfish* peers. It does not use any tamper-resistant hardware, nor does it require an online, interactive authority to be involved in every communication and payment activity. Instead, it explores the profitability principle in packet relaying, and decomposes end-to-end transactions into a manageable series of per-hop transactions. The payment scheme is lightweight, allows intra-payer payment aggregation, and is cheat-resistant against false claim, payment refusal, overspending, and double-spending. Our scheme furthers the idea of PTM [7], without introducing too much network overhead and extra hardware. Our scheme is based on an idea in PayWord [27], but our unique hash-chain construction (i.e. depending on the payer's private-key and the payee's identity) takes full advantage of IBC-powered wireless ad hoc networks, where identity usually is the only means to identify peers, and peer secrecy and wealth are all based on the extracted private-key. An IBC and threshold-based key distribution scheme is briefly outlined in [28] independently, but our work focuses more on peer collaboration rather than key distribution. Also, IBC-based schemes are considered in other contexts such as grid computing [29].

6   Conclusions

Peer collaborations is essential in wireless ad hoc networks due to the lack of infrastructure support; however, voluntary collaboration is found to be too optimistic in practice. In this paper, based on the latest advances in IBC to ensure information confidentiality, integrity, and authenticity, we have designed a hash-chain-based micropayment scheme to stimulate and compensate collaborative peers. The profitability principle and the decomposition approach are generic, and can be applied to other contexts. Our future work will focus on the competitive pricing of selfish peers, especially when relayed data are cacheable at relaying peers for future requests from other peers.

References

1. C. Perkins (ed). *Ad hoc networking*. Addison-Wesley, 2001.
2. Z. Haas, J. Deng, B. Liang, P. Papadimitatos, and S. Sajama. Wireless ad hoc networks. in J. Proakis (ed) *Encyclopedia of Telecommunications*, 2002.
3. R. Ramanathan and J. Redi. A brief overview of ad hoc networks: challenges and directions. *IEEE Comm. Magazine*, 40(5):20–22, 2002.

4. Z. Haas, M. Gerla, D. Johnson, C. Perkins, M. Pursley, M Steenstrup, and C.-K. Toh (eds). Special issue on wireless ad hoc networks. *IEEE Journal on Selected Areas in Comm.*, 17(8), 1999.

5. S. Micali, T. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. *Proc. 6th ACM Mobile Comp. & Netw. (MobiCom)*, pp. 255–265, 2000.

6. Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. *Proc. 6th ACM MobiCom*, pp. 275–283, 2000.

7. L. Buttyan and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. *Proc. 1st ACM Ad Hoc Netw. & Comp. (MobiHoc)*, pp. 87–96, 2000.

8. S. Buchegger and J. Le Boudec. Performance analysis of the confidant protocol: cooperation of nodes - fairness in distributed ad hoc networks. *Proc. 3rd ACM MobiHoc*, pp. 226–236, 2002.

9. P. Michiardi and R. Movla. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. *Proc. 6th IFIP Conf. on Comm. & Multimedia Security*, pp. 107–121, 2002.

10. M. Jakobsson, J.-P. Hubaux, and L. Buttyan. A micropayment scheme encouraging collaboration in multi-hop cellular networks. *Proc. 7th IFCA Financial Cryptography (FC'03)*, 2003.

11. S. Zhong, J. Chen, and Y. Yang. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. *Proc. of 22nd IEEE Infocom*, pp. 1987–1997, 2003.

12. N. Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. A charging and rewarding scheme for packet forwarding in multi-hop cellular networks. *Proc. 4th ACM MobiHoc*, pp. 13–24, 2003.

13. M. Gagnee. Identity-based encryption: a survey. *RSA Labs Cryptobytes*, 6(1):10–19, 2003.

14. L. Buttyan and J.-P. Hubaux (Eds). Report on a working session on security in wireless ad hoc networks. *ACM Mobile Comp. & Comm. Review*, 7(1):74–94, 2003.

15. A. Shamir. Identity-based cryptosystems and signature schemes. *Proc. 4th IACR Conf. on Cryptology (Crypto'84)*, pp. 47–53, 1984.

16. D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. *Proc. 21st IACR Crypto*, pp. 213–229, 2001.

17. L. Cai, J. Pan, X. Shen, and J.W. Mark. Prompting identity-based key management in wireless ad hoc networks. `http://bbcr.uwaterloo.ca/~cai/tr-ibc.pdf`, 2003.

18. L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, 1999.

19. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. *Proc. 3rd IACR AsiaCrypt*, pp. 548–566, 2002.

20. J.-P. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. *Proc. 2nd ACM MobiHoc*, pp. 146–155, 2001.

21. G. Montenegro and C. Castelluccia. Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses. *Proc. 9th ISOC Netw. & Dist. Syst. Security (NDSS)*, 2002.

22. Y.-C. Hu, A. Perrig, and D. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Proc. 8th ACM MobiCom*, pp. 12–23, 2002.

23. P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. *Proc. SCS Comm. Netw. & Dist. Syst. (CNDS)*, 2002.

24. Y.-C. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing in mobile wireless ad hoc networks. *Proc. 4th IEEE Mobile Comp. Syst. & Appl. (WMCSA)*, pp. 3–13, 2002.

25. K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer. A secure routing protocol for ad hoc networks. *Proc. 10th IEEE Netw. Prot. (ICNP)*, pp. 78–87, 2002.

26. R. Rivest. Electronic lottery tickets as micropayments. *Proc. 1st IFCA FC*, 1997.

27. R. Rivest and A. Shamir. PayWord and MicroMint: two simple micropayment schemes. *Proc. Int'l Workshop on Security Prot.*, pp. 69–87, 1997.

28. A. Khalili, J. Katz, and W. Arbaugh. Toward secure key distribution in truly ad-hoc networks. *Proc. IEEE Security & Assurance in Ad-Hoc Netw. (SAINT)*, pp. 342–346, 2003.

29. T. Stading. Secure communication in a distributed system using identity based encryption. *Proc. 3rd IEEE/ACM Clus. Comp. & Grid (CCGRID)*, pp. 414–420, 2003.