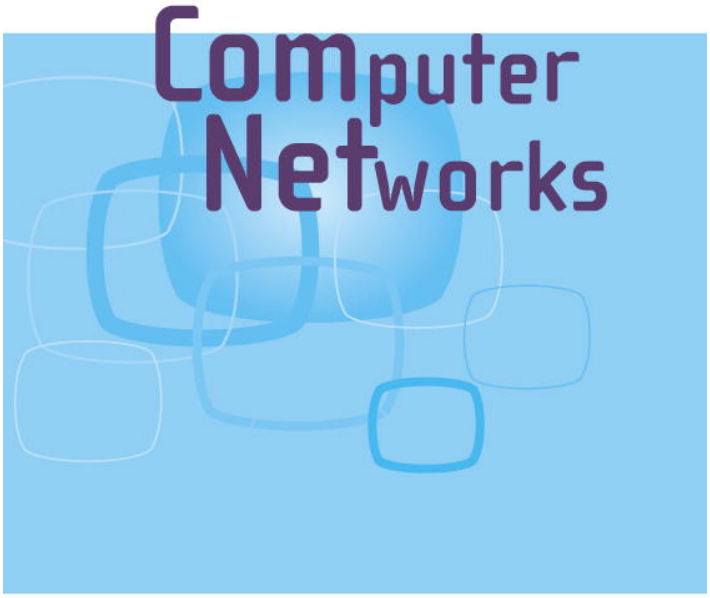
Volume 51 Issue 3 21 February 2007 ISSN 1389-1286



Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 853–865
Computer Networks
www.elsevier.com/locate/comnet

Identity-based secure collaboration in wireless ad hoc networks

Jianping Pan [a,*], Lin Cai [b], Xuemin (Sherman) Shen [c], Jon W. Mark [c]

[a] Department of Computer Science, University of Victoria, Victoria, BC, Canada V8W 3P6
[b] Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada V8W 3P6
[c] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada N2L 3G1

Received 1 May 2006; accepted 10 May 2006
Available online 21 July 2006

Responsible Editor: Dr. R. Boutaba

Abstract

Voluntary peer collaboration is often assumed in media access, route discovery, packet forwarding, and upper-layer protocols designed for wireless ad hoc networks. This assumption has been seriously challenged when 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 in ad hoc networks.

Keywords: Wireless ad hoc networks; Peer collaboration; Identity-based cryptography

1. Introduction

Wireless ad hoc networks are self-organized systems without relying on any preexisting, fixed communication infrastructures, so any peer may assist the communication that is vital for other peers by relaying their packets. Ad hoc networks, which have attracted much attention in recent years [3,4], are especially attractive when infrastructures are too expensive to build, or too vulnerable to maintain [1,2]. *Voluntary collaboration* is often assumed among all involved peers, which is acceptable when these 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 peers are autonomous, selfish, or malicious in large-scale, heterogeneous networks. For example, if battery-powered peers relay packets for others, they are one-step closer to running out of their energy, which is undesirable from a selfish standpoint, since later they may have insufficient energy for their own packets.

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

* Corresponding author. Tel.: +1 250 472 5796.
E-mail address: pan@uvic.ca (J. Pan).

1389-1286/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comnet.2006.05.012

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 others (due to higher interference) or even by itself (due to higher energy consumption). Hence, collaborations among neighbor peers are essential in ad hoc networks.

The desire to collaborate in 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 information exchange 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 Section 6 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 ad hoc networks, where public-key infrastructures (PKIs) or CA hierarchies are also expensive to build and vulnerable to maintain in general. 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 relay packets for others.

The remainder of this paper is organized as follows. In Section 2, we present the model of ad hoc networks and their security requirements. Identity-based key management is presented in Section 3. In Section 4, we design an IBC-based micropayment scheme to stimulate and compensate collaborative peers. Through the performance studies in Section 5, we demonstrate that profitable collaboration is a preferable strategy if it is properly enforced. Section 6 reviews related work, and Section 7 concludes this paper.

2. System model

2.1. Ad hoc networks

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

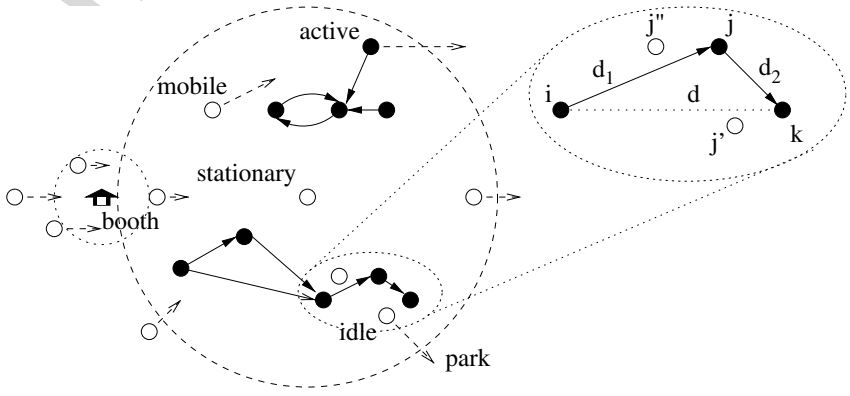


Fig. 1. Relaying in wireless ad hoc networks.

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). However, there are no physical barriers around the vicinity, and peers can join or leave systems at any locations. Without any centralized online authorities, peers can remain stationary or mobile, keep idle (unfilled dots) or active (filled dots), and assist communications among 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 at distance d away. i can have two strategies: (1) i transmits b to k directly, and consumes energy $e_i^t(b,d) = (t_1 + t_2 d^{n(d)})b$, where $2 \leqslant n(d) \leqslant 6$ is the path loss exponent, and t_1 and t_2 are the coefficients of distance-independent and distance-related energy consumption, respectively. However, i may be prevented from doing so when $d > D$ and D is the maximum transmission range of i, or direct communications of i and k impose strong interference to other peers near them. (2) When there is a third peer j between i and k, i may request 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. However, 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 (e.g., by appearing in sleep mode or leaving the vicinity), since j has to sacrifice its own resources for the benefit of others. But as a selfish peer, j may wish other peers (including i and k) to relay for itself to conserve its energy.

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 inversely 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.

2.2. Security requirements

Many security threats appear in 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 ad hoc 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.

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 (j' still has higher profit than j, since it is almost free for j' to obtain b). 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.

3. Identity-based key management

The concept of identity-based cryptography (IBC) was first introduced by Shamir two decades ago [15]; however, non-mediated IBC-based encryption (IBE) is very challenging, and it is only recently that practical IBE schemes appeared. 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). Since then, many new IBC-based encryption and signature schemes (some even without ROM [17]) have been proposed and implemented.

3.1. System setup

Before an IBC-powered wireless ad hoc network becomes fully functional (i.e., allowing peers to join the system and request keying), an offline PKG first picks a random master-key $x \in Z_q$ (q is a prime and Z_q is an algebraic field) and a bilinear mapping $f: G \times G \to Z_q$. f is defined on the points of an elliptic curve (as a group G), and has the following property that for any $P, Q \in G$ and for any integer a and b:

$$f(aP, bQ) = f(P, bQ)^a = f(aP, Q)^b = f(P, Q)^{ab}. \quad (1)$$

The PKG then picks a random generator P, and publishes P, xP, f and four chosen cryptographic hash functions as the public system parameters. These hash functions, which will be explained shortly, are used to hash an arbitrary identity (e.g., any ASCII strings) to a point on the elliptic curve (H_1), to achieve security against chosen ciphertext attacks (H_2 and H_3), and to encrypt plaintext (H_4), respectively. The PKG should keep x secret, and no one else can derive x even when they have both P and xP.

A lot of offline entities (e.g., the ticketing booth of a recreation park) can assume the role of PKG, as long as they can keep the master-key secret and extract private-keys from the master-key for peers joining the system and requesting to be keyed. Once the private-key is extracted, a peer has no need to communicate with the PKG (nor to keep the PKG online), unless the peer wants to propose a new identity. Also, the offline PKG can key peers in batch (e.g., only during normal business hours), since peers can receive regular, encrypted information even before they request keying. Compared with an online PKI, the offline PKG has many advantages in wireless ad hoc networks. With a PKI, whenever a peer k joins a system, the PKI should verify the binding of the public-key of k and its identity, and broadcast the authenticated public-key to all existing peers, or keep the public-key in a central directory for queries from other peers. No matter when another peer i wants to communicate with k, i has to obtain both the identity and the public-key of k, and i should have a way of verifying the public-key, which creates extra overhead in energy-constrained systems that rely on radio technologies to exchange not only user data but also their identities and keys.

3.2. Peer keying

When a peer k joins an IBC-powered wireless ad hoc network, k proposes a system-wide unique identity id_k (or the PKG appends a timestamp or sequence number to peer identity). The PKG obtains a corresponding point $Q = H_1(id_k)$ on the elliptic curve by hashing id_k, and extracts k's private-key $pk_k = xQ$ from the master-key x. id_k can be the email address of k, concatenated with temporal or spatial properties (e.g., *a@b.com@date@site*). Identity ownership should be easily verified, e.g., by short-range encounters [18] when peers passing by the PKG or by sending a request-to-confirm email to *a@b.com*. pk_k is conveyed back to k in a secure, out-of-band side channel (e.g., through the ticketing process at a recreation park); the system parameters are periodically broadcast by the PKG (e.g., through public announcement). To fight against identity theft or spoofing, the PKG should not extract private-keys more than once for the same identity even claimed by the same entity; instead, by using timestamp or sequence number, the entire identity space is always collision-free and forward-secure.

The security of the entire system relies on the master-key x kept by the PKG, since the private-key of all peers in IBC-based wireless ad hoc networks can be derived from x. To reduce the risk of total-exposure even if the PKG is compromised and to address the concern of key escrow for peers with a new PKG, x can be distributed in a t-of-n manner to a group of n PKGs by applying threshold cryptography (TC) techniques [19]. With TC, k

thereby derives pk_k alone by combining pk_k^t obtained from any t PKG_t. Unless there are more than t unknowingly-compromised or bogus PKGs, the secrecy of all peers and their private-key are still preserved.

To support a large entity population, Gentry and Silverberg [20] extended the BF-IBE scheme with a hierarchical PKG structure (GS-HIBC), where a lower-level PKG inherits the identities of its ancestors and obtains its master-key from the parent PKG. In HIBC-powered systems, peers are identified by a tuple of identities, corresponding to their location in the PKG hierarchy, which is also their localized public-key. With HIBC, a peer can easily roam from one ad hoc network to another, and communicate with peers in other networks, by just knowing their identities and the system parameters of the root PKG (not the PKG of other peers). For simplicity, we focus on keying with a single PKG, and the schemes can be extended for t-of-n or hierarchical PKGs.

3.3. Key maintenance

In identity-based schemes, the public-key of a peer is exactly its identity or a known transformation of the identity. Hence, a peer can receive regular information encrypted with its identity from other peers even before the peer has obtained its private-key from the PKG. This unique feature allows asynchronous communications in wireless ad hoc networks, where autonomous peers can be in active, idle or sleep state periodically without global synchronization to conserve energy. Also, this feature reduces the cost of operating the offline PKG, since peers can request keying in batch only after they are actively and willingly involved in receiving information from other peers and when the PKG goes online according to its own schedule. In contrast, in SKC or regular PKC systems, peers have to establish pairwise shared-keys or obtain public-key and private-key pairs way before any secure communications can happen; i.e., keying is always mandatory and proactive for all peers, even if they eventually have no secure communications throughout the validity period of their keys in these systems.

Once a peer obtains its private-key extracted from its identity and the system parameters, the peer can decrypt received information encrypted with its identity, authenticate itself to other peers, and sign outgoing messages. Also, peers can bootstrap shared-keys or derive session-keys from their identity-based private-keys for symmetric security procedures. Once bootstrapped, symmetric procedures have much less overhead than their asymmetric counterparts. Depending on the definition of peer identity, a peer, as well as the PKG, can determine the lifetime of its private-key. For example, a peer can propose the same identity (e.g., *username*) to systems with different parameters (i.e., the peer will have different private-keys in different systems); even if its private-key is compromised in one system, the information exposure is confined to that system. A peer can propose an ephemeral identity (e.g., *user@time*); even if its private-key is compromised at a certain time, the peer can request a new private-key with a partially-updated identity in *time* portion, without totally losing its identity or forcedly leaving the system. When necessary, a peer can proactively refresh its identity (e.g., *user@date*) with the PKG and remain forward-secure even if its current private-key is captured and compromised by adversaries. To deal with an unknown PKG, a peer can propose a temporary identity (e.g., *user@site*) to a newly-encountered system, while maintaining credentials with other well-known systems. Further, a peer can request keying with multiple or hierarchical PKGs to reduce its exposure due to compromised PKGs, and to ease its concern of key escrow by untrusted PKGs.

The PKG, on the other hand, can also control the validity of peer identities and extracted private-keys. For example, a peer should have a way of proving its identity ownership (e.g., *a@b.com*) or accept assigned identities (e.g., prepaid personal identification number). A peer is uniquely identified by its identity, which can be both time and location invariant within the system. No matter how the peer changes its location and status in the system, it solely relies on its identity to receive information and communicate with other peers. In addition, its identity is related to its reputation (e.g., cooperativeness in relaying) and wealth (e.g., collected credits for its cooperation) in the system. If a peer is found greedy and always fails to relay for other peers, this fact can be taken into account when the peer is in need of relaying by other peers. If a peer is found malicious, either persistently or opportunistically, the peer can be excluded from the system by identity blacklisting or key expiring (e.g., the PKG enforces an identity upgrade and refuses to key compromised peers). The PKG can have differentiated policies, e.g., extracting keys of *user@month* for well-established or reputable peers (e.g., a

monthly pass to a recreation park) and of *user@day* for new or ill-behaving peers (e.g., a one-time ticket). Certainly, the PKG can enforce a system-wide rekeying after a long time-period by updating the master-key and the system parameters, and peers will need to contact the PKG again to extract their new private-key.

4. Secure peer collaboration

With IBC-based schemes, peers in ad hoc networks can communicate securely without relying on PKIs, CA hierarchies, key directories, online authorities, or pairwise prearranged secrets among all involved peers. 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 destination-payer model; other payment models (e.g., source-payer) can be accommodated by prefixing application-layer payments (i.e., sources pay destinations directly) to our scheme.

4.1. 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 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 $CCFM\{id_{j+1}, tn, id_{pkg}, id_j, S_{pk_{pkg}}^{tn}, et\}_{sk_{pkg,j+1}}$.

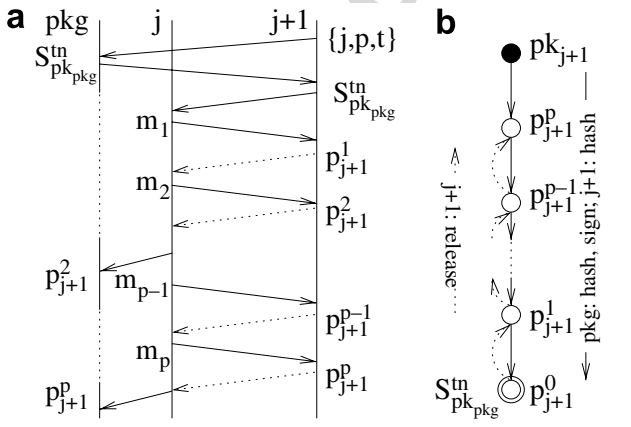


Fig. 2. Per-by-hop transactions: (a) payment schedule; (b) payment chain.

$j+1$ 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 the format of $HMSG\{id_{j+1}, tn, id_j, m_i, et\}_{sk_{j,j+1}}$, and after the authenticity of m_i is verified, $j+1$ releases the hash-chain gradually in a reverse order (i.e., $p_1, p_2, \ldots, p^p$) 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 corresponding 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 relaying evidence.

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

In our design, $j+1$ cannot deny released payments after it receives m_i from j (except for, 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 its 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 non-existent relaying and payments, their overall wealth does not increase. Therefore, selfish peers have no incentives to collude with others 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^0_{j+1}, the PKG can easily find the proper amount j should claim by hashing p^i_{j+1} 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 $S^{tn}_{pk_{pkg}}$, so j has to claim received payments before expiry.

4.2. End-to-end transactions

As shown in Fig. 3(a), 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 peer 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 is profitable. Within a time window, a peer does not respond to a solicitation that is a subset of its own. In Fig. 3(a), 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. The reason for this may be j'' is too close to j (see

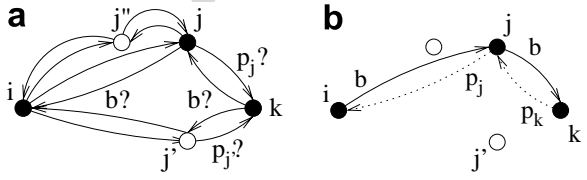


Fig. 3. End-to-end transactions: (a) relay negotiation; (b) relay commitment.

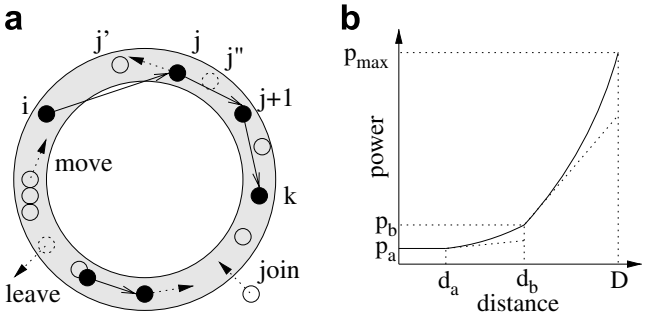


Fig. 4. Simulation configurations: (a) network topology; (b) power consumption.

Fig. 4(b)), j'' expects higher profit, or j'' has less remaining energy. Based on its profit strategy, j offers b to k at a price p_j, which is profitable for j and supposedly acceptable for k in $RSPS\{\{id_i, sn, id_k, if(b)\}_{pk_k}, id_j, p_j\}_{sk_{j,k}}$. Certainly, j has to offer b at a competitive price, since there are other relaying candidates competing with j and communicating with k securely and exclusively; otherwise, k prefers to deal with other peers 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. 3(b). Source peer i should prepare b in a proper format for relaying, e.g., $\{\{m_1\}_{pk_i}, \{m_2\}_{pk_i}, \ldots, \{m_n\}_{pk_i}\}$, where $\{\cdot\}_{pk_i}$ implies these messages are protected in an end-to-end manner by i's signature (or signcryption if confidentiality is also required), 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 in this example) 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 accordingly. 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 by nearby peers due to other requests.

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.

4.3. Collaboration strategies

With our security and collaboration measures, peers can have three basic strategies. First, a *voluntary* peer relays for all other peers. Voluntary peers will attract a lot of selfish peers, and probably run out of their energy very quickly. 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. However, selfish peers may wish voluntary and collaborative peers to relay for them, either for free or at a very low price.

There are many alternatives to these strategies. For instance, a peer can selectively collaborate with peers being 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. To understand the performance of these strategies for individual peers and for the entire system, we conduct some simulation-based studies and report numerical results in the next section.

5. Performance evaluation

5.1. Evaluation approach

We consider a wireless ad hoc network with the topology shown in Fig. 4(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 networks with 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 ad hoc networks. Location preference in a general topology can be compensated by peer density, preferable pricing, and other traditional means.

At any time, peers can join or leave the network overseen by a PKG. When a peer with a certain amount of initial energy joins the network, it obtains its private-key corresponding to the proposed identity from the PKG, and deposits a certain amount of monetary credits at the PKG to compensate relaying peers (and the PKG for control traffic). 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. 4(b), when distance d is less than a threshold d_a, the transmission power consumption remains constant, i.e., $n(d) = 0$ when $0 < d \leqslant d_a$, and relaying does not offer additional cost-saving. Once $d > d_a$, the distance-related transmission power consumption becomes dominant. When $d_a < d \leqslant d_b$, 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., $n(d) \geqslant 4$. The maximum output power ($p_{\max}$) of its transmitter limits the distance that a peer can reach, so $d \leqslant D$. Here, $D < 2R$, i.e., peers cannot always communicate with other peers directly.

CiC peers equally share the cost-saving at downstream peers due to their relaying. Although a peer has no exact knowledge of the cost-saving at other peers, within a competitive pricing and auction framework, such a goal is approachable. For simplicity, in our simulation, we assume CiC peers know the location of source and downstream peers (e.g., through their location-based identity), and calculate and share the cost-saving at downstream peers independently.

5.2. 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 in the network. A peer requests data of size 1–100 unit from other peers randomly, if it has enough remaining energy to receive data and enough available credits to compensate relaying peers when necessary. We consider four peer scenarios listed in Table 1.

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 the information is more valuable 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 system initialization. Also, 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.

Table 1
Peer demography

No.	Peer %			Demographic scenario
	V	*CiC*	*SS*	
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

Fig. 5(b) shows 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 consumed. 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 have to eventually pay higher cost to transfer data over greater distances. *CiC* peers, on the other hand, accumulate credits when they relay for others, and trade for energy when necessary; they conserve energy much better than *V* and *SS* peers.

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 maintain the remaining energy, *CiC* peers obtain much more information than *V* and *SS* peers. Combining Figs. 5(b) and (c), it is easy to see peer collaborations increase system utility with more obtained information and less consumed energy. This observation is confirmed by the numbers listed in Table 2. 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 that *S* peers indeed have a much lower utility than *CiC* peers.

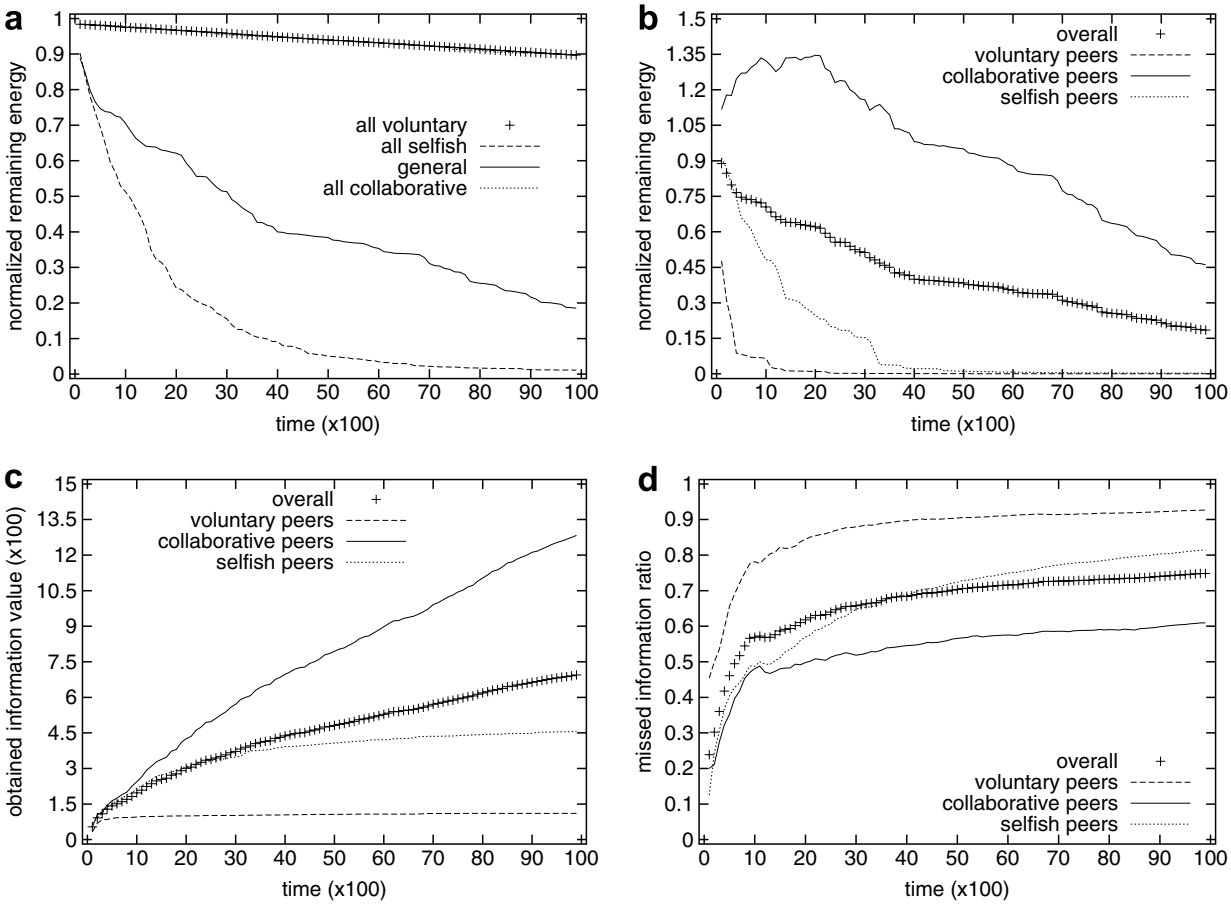


Fig. 5. Numerical results for per-peer performance metrics: (a) different demographic scenarios; (b) general demographic scenario; (c) obtained information value; (d) missed information ratio.

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. Once most *V* peers are out of energy, *SS* peers suffer a much higher information miss ratio as well.

Table 2
System performance metrics

Scenario		Consumed energy (%)	Obtained information	Average utility
III	Overall	81.5	694.508	852.157
	V	100.0	110.550	110.550
	CiC	53.9	1283.308	2380.905
	S	99.7	455.619	456.990

Through these performance studies, it is concluded that when security and collaboration measures are properly enforced, profitable collaboration is a preferable strategy for all peers in ad hoc networks. In addition, with profitable collaboration, system utility will increase when peers have maximized their potential profit, which justifies the motive for ad hoc networks to adopt these measures.

6. Related work

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 considerable research efforts toward securing information exchange in such systems [14,19,21–26]. Also, the assumption of voluntary collaboration in 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 to transfer receipts. Besides fully-distributed ad hoc networks, peer collaborations are 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 [27]. 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* collaborations 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 tamper-resistant hardware. Our scheme is based on an idea in PayWord [28], 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 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 [29] independently, but our work focuses more on peer collaboration rather than key distribution. In addition, IBC-based schemes are considered in the contexts other than ad hoc networks [30].

7. Conclusions

Peer collaborations are 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.

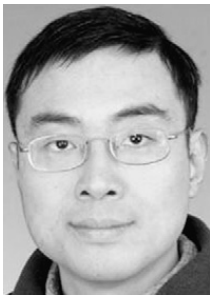
Acknowledgement

This work has been supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] C. Perkins (Ed.), Ad hoc Networking, Addison-Wesley, 2001.
[2] Z. Haas, J. Deng, B. Liang, P. Papadimitatos, S. Sajama, Wireless Ad hoc Networks, in: J. Proakis (Ed.), Encyclopedia of Telecommunications, Wiley, 2002.
[3] R. Ramanathan, J. Redi, A brief overview of ad hoc networks: challenges and directions, IEEE Commun. Mag. 40 (5) (2002) 20–22.
[4] Z. Haas, M. Gerla, D. Johnson, C. Perkins, M. Pursley, M. Steenstrup, C.-K. Toh (Eds.)IEEE J. Selected Areas Commun. 17 (8) (1999) 1329–1531 (Special issue on wireless ad hoc networks).
[5] S. Micali, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the 6th ACM MobiCom, 2000, pp. 255–265.
[6] Y. Zhang, W. Lee, Intrusion detection in wireless ad-hoc networks, in: Proceedings of the 6th ACM MobiCom, 2000, pp. 275–283.
[7] L. Buttyan, J.-P. Hubaux, Enforcing service availability in mobile ad-hoc WANs, in: Proceedings of the 1st ACM MobiHoc, 2000, pp. 87–96.
[8] S. Buchegger, J. Le Boudec, Performance analysis of the confidant protocol: cooperation of nodes – fairness in distributed ad hoc networks, in: Proceedings of the 3rd MobiHoc, 2002, pp. 226–236.
[9] P. Michiardi, R. Movla, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Proceedings of the 6th IFIP Conference on Communications and Multimedia Security, 2002, pp. 107–121.
[10] M. Jakobsson, J.-P. Hubaux, L. Buttyan, A micropayment scheme encouraging collaboration in multi-hop cellular

networks, in: Proceedings of the 7th Financial Cryptography (FC'03), 2003.
[11] S. Zhong, J. Chen, Y. Yang. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks, in: Proceedings of the 22nd IEEE Infocom, 2003, pp. 1987–1997.
[12] N. Salem, L. Buttyan, J.-P. Hubaux, M. Jakobsson, A charging and rewarding scheme for packet forwarding in multi-hop cellular networks, in: Proceedings of the 4th MobiHoc, 2003, pp. 13–24.
[13] M. Gagnee, Identity-based encryption: a survey, RSA Labs Cryptobytes 6 (1) (2003) 10–19.
[14] L. Buttyan, J.-P. Hubaux (Eds.), Report on a working session on security in wireless ad hoc networks, Mobile Comput. Commun. Rev. 7(1) (2003) 74–94.
[15] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proceedings of the 4th IACR Conference on Cryptology (Crypto'84), 1984, pp. 47–53.
[16] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: Proceedings of the 21st IACR Crypto, 2001, pp. 213–229.
[17] D. Boneh, X. Boyen, Secure identity based encryption without random oracles, in: Proceedings of 24th IACR Cryptology (Crypto'04), 2004.
[18] S. Capkun, J.-P. Hubaux, L. Buttyan, Mobility helps security in ad hoc networks, in: Proceedings of 4th ACM Mobile Ad Hoc Networking and Computing (MobiHoc'03), 2003, pp. 46–56.
[19] L. Zhou, Z. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24–30.
[20] C. Gentry, A. Silverberg, Hierarchical ID-based cryptography, in: Proceedings of the 3rd AsiaCrypt, 2002, pp. 548–566.
[21] J.-P. Hubaux, L. Buttyan, S. Capkun, The quest for security in mobile ad hoc networks, in: Proceedings of the 2nd ACM MobiHoc, 2001, pp. 146–155.
[22] G. Montenegro, C. Castelluccia, Statistically unique and cryptographically verifiable (SUCV) identifiers and addresses, in: Proceedings of the 9th ISOC Conference on Network & Distributed Systems Security (NDSS'02), 2002.
[23] Y.-C. Hu, A. Perrig, D. Johnson, Ariadne: a secure on-demand routing protocol for ad hoc networks, in: Proceedings of the 8th ACM MobiCom, 2002, pp. 12–23.
[24] P. Papadimitratos, Z. Haas, Secure routing for mobile ad hoc networks, in: Proceedings of the SCS Conference on Communication Networks & Distributed Systems (CNDS'02), 2002.
[25] Y.-C. Hu, D. Johnson, A. Perrig, SEAD: secure efficient distance vector routing in mobile wireless ad hoc networks, in: Proceedings of the 4th IEEE WMCSA, 2002, pp. 3–13.
[26] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, E. Belding-Royer, A secure routing protocol for ad hoc networks, in: Proceedings of the 10th IEEE ICNP, 2002, pp. 78–87.
[27] R. Rivest, Electronic lottery tickets as micropayments, in: Proceedings of 1st IFCA FC'97, 1997.
[28] R. Rivest, A. Shamir, PayWord and MicroMint: two simple micropayment schemes, in: Proceedings of the International Workshop on Security Protocols, 1997, pp. 69–87.
[29] A. Khalili, J. Katz, W. Arbaugh, Toward secure key distribution in truly ad-hoc networks, in: Proceedings of the IEEE Security and Assurance in Ad-Hoc Networks at International Symposium on Applications and the Internet (SAINT'03), 2003, pp. 342–346.
[30] T. Stading, Secure communication in a distributed system using identity based encryption, in: Proceedings of the 3rd IEEE/ACM Cluster Computing and Grid (CCGRID'03), 2003, pp. 414–420.



Jianping Pan is currently an assistant professor of computer science at the University of Victoria, British Columbia, Canada. He received his Bachelor's and Ph.D. degrees in computer science from Southeast University, Nanjing, China in 1994 and 1998, respectively. From 1999 to 2001, he was a postdoctoral fellow and then a research associate at the University of Waterloo, Ontario, Canada; from 2001 to 2005, he was a member of research staff at Fujitsu Labs and then a research scientist at NTT MCL in Silicon Valley, California, USA. His area of specialization is distributed systems and computer networks, and his recent research interests include protocols for advanced networking, performance analysis of networked systems, and applied network security. He is a member of the ACM and the IEEE.

Lin Cai received the M.A.Sc. and Ph.D. degrees (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, Canada, in 2002 and 2005, respectively. Since July 2005, she has been an Assistant Professor in the Department of Electrical and Computer Engineering at the University of Victoria, British Columbia, Canada. Her research interests span several areas in wireless communications and networking, with a focus on network protocol and architecture design supporting emerging multimedia traffic over wireless, mobile, ad hoc, and sensor networks. She serves as the Associate Editor for EURASIP Journal on Wireless Communications and Networking, and International Journal of Sensor Networks (IJSNet). She is a member of IEEE and ACM.

Xuemin (Sherman) Shen received the B.Sc. (1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. From September 1990 to September 1993, he was first with the Howard University, Washington D.C., and then the University of Alberta, Edmonton (Canada). Since October 1993, he has been with the Department of Electrical and Computer Engineering, University of Waterloo, Canada, where he is a Professor. His research focuses on mobility and resource management in interconnected wireless/wireline networks, UWB wireless communications systems, wireless security, and ad hoc and sensor networks. He is a coauthor of two books, an editor of 10 journal Special issues, and

has published more than 150 papers in wireless communications and networks, control and filtering.

He was the Technical Co-Chair for IEEE Globecom'03 Symposium on Next Generation Networks and Internet, and ISPAN'04. He serves as the Associate Editor for IEEE Transactions on Wireless Communications; IEEE Transactions on Vehicular Technology; ACM Wireless Networks; Computer Networks; Dynamics of Continuous, Discrete and Impulsive – Series B: Applications and Algorithms; Wireless Communications and Mobile Computing (Wiley); and International Journal Computer and Applications. He also serves as Guest Editor for IEEE JSAC, IEEE Wireless Communications, and IEEE Communications Magazine. He received the Premier's Research Excellence Award (PREA) from the Province of Ontario, Canada for demonstrated excellence of scientific and academic contributions in 2003, and the Distinguished Performance Award from the Faculty of Engineering, University of Waterloo, for outstanding contribution in teaching, scholarship and service in 2002. He is a senior member of the IEEE, and a registered Professional Engineer of Ontario, Canada.

Jon W. Mark received the B.A.Sc. degree from the University of Toronto in 1962, and the M.Eng. and Ph.D. degrees from McMaster University in 1968 and 1970, respectively, all in electrical engineering. From 1962 to 1970, he was an engineer and then a senior engineer at Canadian Westinghouse Co. Ltd., Hamilton, Ontario, Canada. In September 1970 he joined the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, where he is currently a Distinguished Professor Emeritus. He served as the Department Chairman during the period July 1984–June 1990. In 1996 he established the Centre for Wireless Communications (CWC) at the University of Waterloo and is currently serving as its founding Director. He had been on sabbatical leave at the following places: IBM Thomas J. Watson Research Center, Yorktown Heights, NY, as a Visiting Research Scientist (1976–77); AT&T Bell Laboratories, Murray Hill, NJ, as a Resident Consultant (1982–83); Laboratoire MASI, Universit Pierre et Marie Curie, Paris France, as an Invited Professor (1990–91); Department of Electrical Engineering, National University of Singapore, as a Visiting Professor (1994–95). He has previously worked in the areas of adaptive equalization, image and video coding, spread spectrum communications, computer communication networks, ATM switch design and traffic management. His current research interests are in broadband wireless communications, resource and mobility management, and cross domain interworking. He recently co-authored the text entitled Wireless Communications and Networking, Prentice-Hall 2003. A Life Fellow of IEEE, he is the recipient of the 2000 Canadian Award for Telecommunications Research and the 2000 Award of Merit of the Education Foundation of the Federation of Chinese Canadian Professionals. He was an editor of IEEE Transactions on Communications (1983–1990), a member of the Inter-Society Steering Committee of the IEEE/ACM Transactions on Networking (1992–2003), a member of the IEEE Communications Society Awards Committee (1995–1998), an editor of Wireless Networks (1993–2004), and an associate editor of Telecommunication Systems (1994–2004).