Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 469076, 10 pages
http://dx.doi.org/10.1155/2013/469076

Research Article

A PEFKS- and CP-ABE-Based Distributed Security Scheme in Interest-Centric Opportunistic Networks

Fei Wang,[1,2] YongJun Xu,[1] Lin Wu,[1,2] Longyijia Li,[3] Dan Liu,[3] and Liehuang Zhu[3]

[1] *Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China*
[2] *University of Chinese Academy of Sciences, Beijing 100049, China*
[3] *School of Computer Science & Technology, Beijing Institute of Technology, Beijing 100081, China*

Correspondence should be addressed to Fei Wang; wangfei@ict.ac.cn

Received 26 December 2012; Accepted 16 March 2013

Academic Editor: Hongsong Zhu

Security is a crucial issue in distributed applications of multihop wireless opportunistic network due to the features of exposed on the fly communication, relaxed end-to-end connectivity, and vague destinations literately. In this paper, we focus on problems of user privacy leakage and end-to-end confidentiality invasion in content-based or interest-centric wireless opportunistic network. And we propose a public-encryption-with-fuzzy-keyword-search- (PEFKS-) and ciphertext-policy-attribute-based-encryption- (CP-ABE-) based distributed security scheme by refining and compromising two-pairing-based encryption, searchable encryption, and attribute-based encryption. Our scheme enables opportunistic forwarding according to fuzzy interests preserving full privacy of users and ensures end-to-end confidentiality with a fine-grained access control strategy in an interest-centric scenario of large-scale wireless opportunistic networks. Finally, we analyze and evaluate the scheme in terms of security and performance.

1. Introduction

Opportunistic network is a type of ad hoc wireless network which has common features of delay tolerant network (DTN), which achieves routing through opportunities of meeting between mobile nodes. It aims to solve the problem of communication in the presence of intermittent network connectivity. And to this end, opportunistic network (OPPNET) has the following features.

(i) Communication is on the fly, thus exposed to all powerful adversary parties trying to spy the privacy of users and steal the information.

(ii) Forwarding decisions are made on the fly based on any possible information from a collapsed network architecture [1], owing to the aim of transmitting a message over any communication gaps.

(iii) Only vague destinations literately exist because a message ought to be sent to a group of nodes according to some principles: deployed near a specific location, equipped with same sensors or actuators, or interested in specific information [2].

Content-based opportunistic network uses content of message which concerns users' interests to make forwarding decisions, and a most popular application scenario is that network nodes which are actually pedestrians look forward to acquiring and sharing information through opportunistic communication with others. Every pedestrian carries one or more portable wireless terminals such as smart phones, tablets, and laptops. More precisely, it is people-centric or interest-centric opportunistic network. In such a scenario, a user can be a subscriber with interests in some topics; he could also be a publisher intending to publish contents about some topics. Security in such type of opportunistic network is a crucial issue. We consider two components of security in opportunistic network: privacy and confidentiality.

First is privacy. In a content-based opportunistic network, interest advertisements from subscribers and published contents from publishers both need to be forwarded based on the interest-oriented information (maybe some indexes, abstracts, keywords, etc.) which are contained in the messages. The routing could be multihop through several intermediate nodes which might not be trusted by subscribers or publishers. The subscribers do not want other

subscribers and intermediate nodes to know their interests. The situation is almost the same as publishers: they do not want other publishers, intermediate nodes, or subscribers that are not designated to obtain the interest orientations of their published contents. However, in precedent research about interest-centric network, forwarding relies on explicit queries or indexes, which leads to possible threat of privacy leakage due to matching between message indexes and users' identities.

Second is end-to-end confidentiality which is considered as a fundamental security requirement. Publishers not only want to impose a ban on the access to the plaintext payload of their published contents, but also want to attach a precise access control strategy to their every message so that only the designated subscribers who have certain credentials or attributes can access the payload. For example, when top layer of some IT company wants to publish a product fault survey, they may make such an access control structure as shown in Figure 1 which means only the department manager of Technology Department or Quality Control Department, staff with management level over 5 or a consultant called Charlie Eppes, could access the survey. However, the reasons of no stable end-to-end connection and group target of a message not only make traditional end-to-end encryption unsuitable, but also increase the difficulty of fine-grained access control on shared data.

In this paper, we propose a *PEFKS*- and *CP-ABE*-based distributed security scheme in interest-centric opportunistic network.

The main contributions of this paper are as follows.

(i) We design a *PEFKS*-based privacy protecting forwarding decision scheme, which on one hand enables subscribers to publish encrypted fuzzy interests and on the other hand enables intermediate nodes to forward messages according to encrypted fuzzy interests. The scheme ensures users' full privacy in the circumstance of opportunistic network and enhances anonymity through fuzzy interests. To the best of our knowledge, we are the first to enable partial match on fuzzy interests in opportunistic network.

(ii) We embed the concept of attribute-based identity into opportunistic network to adapt to the feature of no explicit destinations. Then we design a *CP-ABE*-based confidentiality protecting scheme, in which publishers make and attach an expressive access control strategy to the messages they are about to send. Subscribers whose attribute-based identities satisfy the access control strategy are legalized to decrypt the ciphertext, finally achieving confidentiality with a fine-grained access control strategy on shared data.

(iii) We implement and analyze the security and performance of the schemes and verify the feasibility of our security schemes.

2. Related Work

Related research work is still scarce because security in content-based opportunistic network is a quickly emerging problem and most of the security schemes existing in Internet, wireless sensor networks (WSNs), mobile ad hoc networks (DTN, or MANET) are not suitable.

As far as we are concerned, Lilien et al. [3] were the first to consider security in opportunistic network. They proposed several challenges in privacy and confidentiality of opportunistic network in particular the requirement for end-to-end confidentiality, but they did not propose any possible security solution. What is more, they did not analyze the issue of context privacy or content privacy.

Nguyen et al. proposed a probabilistic routing protocol for ICMAN (intermittently connected mobile ad hoc network) in [4], which indicates the very first idea to protect privacy and confidentiality. In their protocol, if senders want to send messages to receivers, it hashes all the values of message head. Before intermediate node does the partial match, it first calculates its attributes using the same hash functions. Only hash function is used hereby to achieve a relatively computational efficiency, but it is obviously prone to dictionary attack. As for confidentiality, they used the information (evidence/values) that the sender knows about the destination node as keys, so only the destination node can decrypt the cipher messages to get the plain messages in a community scenario. In this scheme the confidentiality is based on assumption that all in-community members can be trusted which obviously cannot be guaranteed in opportunistic network.

In the neighboring area of DTN, a bundle security protocol (BSP) [5] was defined to enhance the security of communications in DTN. In BSP, a confidentiality block is included to enable the encryption of the entire payload at the source and the decryption at the final destination based on the identifier of the destination. It does not enable encryption based on the interests of destinations or partial matches that can be used to make interest-centric forwarding decisions. Those features are thus not enough to satisfy the interest-centric scenario.

Shikfa et al. proposed a scheme for content-based and context-based opportunistic network in [1, 6]. In content-based scenario, they defined a three-level privacy model and two security primitives "secure look-up" and "setup of forwarding tables" and proposed a distributed security scheme based on multiple layer commutative encryption (MLCE) in which r-hop neighbor nodes share keys to encrypt and decrypt messages. There are two disadvantages: one is that only single-word keyword is supported, it is not flexible, and the other is that the number of shared keys will explode when topology changes frequently. In context-based scenario, they replaced identities of classic identity-based encryption (IBE) with attributes contained in context to assure end-to-end confidentiality. Also, they used improved public encryption with keyword search (PEKS) to make forwarding decisions to protect users' privacy. Their scheme is flexible enough to meet the privacy requirements of context-based forwarding. But it only supports strictly limited attributes arrange rules such as ⟨[Mail], [Workplace], [Status]⟩ which is not suitable for content-based forwarding. In addition, the sender cannot apply a fine-grained access control strategy to shared data.

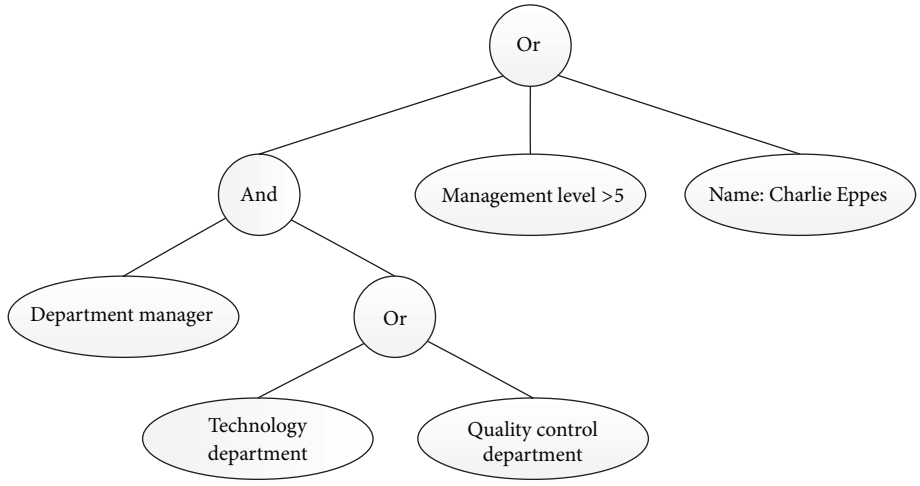

Figure 1: Access policy, for example, in introduction.

There are also other researches concerning security in opportunistic network. As for trust relationship, Li and Das designed a trust-based framework in [7] to more accurately evaluate an encounter's competency met, which can be flexibly integrated with a large family of existing data forwarding protocols. The proposed framework was implemented with PROPHET, demonstrating great effectiveness against "black hole" attacks. But in [7], neither privacy nor confidentiality is considered. Shin et al. presented and implemented AnonySense, a privacy-aware system for realizing pervasive applications based on collaborative, opportunistic sensing by personal devices in [8]. In their system, the sensing tasks and sensor data can be anonymized through the collaboration of Tor network, MIX network and anonymization service (AS) before being reported back. Such a framework achieves great flexibility with users' privacy respected, yet the privacy in opportunistic forwarding is not considered. To improve privacy and confidentiality in opportunistic network, we should mine deeper in modern cryptography.

PEKS was presented by Boneh et al. [9] based on bilinear pairings which makes searching on encrypted data possible. PEKS was improved and used in [1]. But only explicit keywords are not enough to fit in complex application requirements, especially when users know little about the network. When users submit complete queries, they will feel "left in the dark" [10] and have to use a try-and-see approach for finding information. In this respect, fuzzy interests and match of them which can enhance the user interactivity are needed, which current PEKS implemented in opportunistic network cannot achieve. In [11], wildcard-based fuzzy set construction was introduced, but for a word of length l and similarity d quantized by edit distance [12], the size of fuzzy set is $O(l^d)$. In this fuzzy set, many meaningless words that existed bring spatial redundancy. Later, in [13], dictionary-based fuzzy set construction was proposed to improve the efficiency dramatically.

Shikfa introduced IBE and their scheme fits well in context-based opportunistic network. IBE is proposed by Shamir [14] and Boneh and Franklin [15] based on bilinear pairings. It enables resource providers (publishers in opportunistic network) to utilize user's identity as public key without querying for public key certificate online. This feature fits the relaxed-connection environment of opportunistic network very well and was demonstrated in Shikfa's work.

Based on IBE, Sahai and Waters proposed attribute-based encryption or fuzzy identity-based encryption (*ABE*) in 2005 [16]. Research in *ABE* has been hot since then. Su et al. compared *ABE* with IBE and summed up for advanced features in [17]. All these features are very suitable for opportunistic networks. The first is that *ABE* enables resource providers to encrypt messages with only attributes without considering the number or identities in the group, which can reduce the encryption cost on opportunistic network nodes and protect users' privacy in a tailor-made no-explicit-destination environment of opportunistic network. Secondly, only the one whose attribute-based identity satisfying the requirement of cipher text can decrypt the cipher text, which assures end-to-end confidentiality in a relaxed connected environment of opportunistic network. Third is that in *ABE*, users' key was related to random polynomial or random number; thus no collusion is possible among opportunistic network users. The last is that flexible access control strategies such as the AND, OR, NOT, and THRESHOLD of attributes are supported which will dramatically increase the flexibility. The first basic *ABE* [16] scheme only supports threshold access strategy; then researchers developed it and proposed key-policy attribute-based encryption (*KP-ABE*) [18] and ciphertext-policy attribute-based encryption (*CP-ABE*) [19] to achieve more flexible access control strategies. The former enables users to make rules about the messages they are going to receive, and the latter allows senders to make access strategies for ciphertexts.

From the aforementioned work, it could be concluded that none of related research work has achieved privacy or confidentiality with good flexibility in content-based opportunistic network. Some kind of improved PEKS and *ABE* can be our first choice. Therefore we propose a privacy protecting forwarding decision scheme based on *PEFKS* and a confidentiality protecting scheme based on *CP-ABE*.

3. Problem Statement

3.1. Reference Model. The involved nodes of interest-centric opportunistic network are some people working in the same or near places, carrying portable devices with one or more wireless communication interfaces such as Wi-Fi, near field communication (NFC), and Bluetooth. They devote themselves to the opportunistic network system to get information (news, e-mails, gossip, etc.) through multi hop forwarding based on their opportunistic mobility. Their roles in such a system are equal and could work as a subscriber, an intermediate node, and a publisher [20] at the same time. In fact, all users are supposed to be greedy and intend to get without sharing. Therefore, some incentive system exists aiming at leading users to offer their devices' capacity such as storage space and computing power.

Figure 2 depicts the reference model of opportunistic communication in previously mentioned application scenario, in which a subscriber A broadcasts its interest advisements RA, while a publisher C publishes contents PC. Intermediate nodes are responsible for two things: setup of forwarding tables FT according to interest advisements and decision making based on forwarding tables.

To specify the limitation of interest keywords, D_0 is defined as a dictionary containing all valid English words which might be chosen as candidate interests. Every valid user has a subset of candidate keywords W_u^* which would be constant in the lifetime of an opportunistic network. Additionally, all people involved have their own attributes set $Y = \{y_{u,1}, y_{u,2}, \ldots, y_{u,n}\}$ to describe their identities. Users' interests vary over time with the change of hot topics. So interest-centric opportunistic network enables users to update their current interests which all come from W_u^*.

Subscriber's interest advertisement message is composed of two parts: control information CI_A of the message and identity ID_A of A, expressed as $RA = [CI_A, ID_A]$. Without considering security of the network, CI_A is a sub set of W_A^*. ID_A is identity of subscriber A.

Publisher's published message is composed of three parts: control information, payload, and access policy, which could be represented as $PC = [CI_C, P_C, A_{P_C}]$. CI_C represents publisher-defined keywords which can be used as an index of the payload P_C. A_{P_C} is access policy of P_C which supports AND, OR, and THRESHOLD of interests. In this paper we refer to the definition of access policy from [19] directly.

An intermediate node's kth record in forwarding table is composed of two parts: routing information and set of identities of subscribers who are interested in the routing information. We express it like $FT[k] = [RI_k, SID_k]$. RI_k is the routing information and SID_k is the set of identities of subscribers who are interested in the routing information. What is more, every intermediate node will maintain a message list $List_B = \{PC_{B,1}, PC_{B,2}, \ldots, PC_{B,L_B}\}$ containing the messages to be forwarded with the size of L_B.

3.2. Threat Model. In this paper, we focus on two kinds of threats: one is user privacy leakage through indexing information embedded in interest advertisements and published contents, and the other is information stealing from published contents. The threat model is illustrated in Figure 3.

The first kind of threats aims at acquiring and recording the trends of users' interests and published contents which are considered as privacy. The executors could be an adversary or a malicious authenticated user. Here we suppose that it is extremely hard to pass the authentication for an adversary; thus neither impersonation nor forgery is possible. As formor type, the main attacking measure is eavesdropping and brute force attack. Adversary, whose computation capability is powerful, would sniff all the packets in its communication range and try to reveal the privacy. As the latter, executors have normal computation power and act just like the normal users by advertising, forwarding, and publishing. What is more, they would advertise or publish some specific topics to confuse and pry into privacy.

The second kind of threats could also be performed by the afoementioned two kinds of executors. An adversary would keep attacking with brute force, and malicious users would advertise interests as many as possible on purpose and try to find some clues of personal information.

3.3. Design Goals. There are two goals we would like to achieve in our research.

(i) We intend to design a privacy preserving forwarding decision scheme, which on one hand enables subscribers to publish encrypted fuzzy interests on the other hand enables intermediate nodes to forward messages according to encrypted fuzzy interests. The scheme can assure users' full privacy in the circumstance of opportunistic network and enhance anonymity through fuzzy interests.

(ii) We want to embed the concept of attribute-based identity into opportunistic network to adapt to the feature of no explicit destinations. And we intend to design a confidentiality preserving scheme with a fine-grained access control strategy on shared data, in which publishers make and attach an expressive access control strategy to the messages they are about to send. Only subscribers whose attribute-based identities satisfy the access control strategy are legalized to decrypt the ciphertext.

4. Proposed Scheme

In this chapter we will firstly introduce the security preliminaries needed in the demonstration of our scheme in Section 4.1. Then our *PEFKS*- and *CP-ABE*-based distributed security scheme will be described in Sections 4.2 and 4.3.

4.1. Preliminaries

(1) PEKS will be used in in forwarding decision scheme to protect privacy. It consists of three preliminaries: PEKS, Trapdoor, and Test.

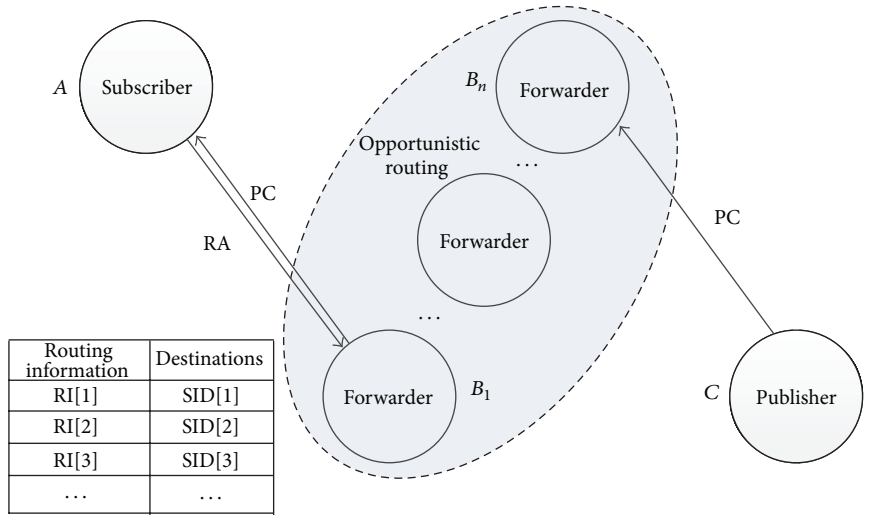

Figure 2: Opportunistic network application scenario model.

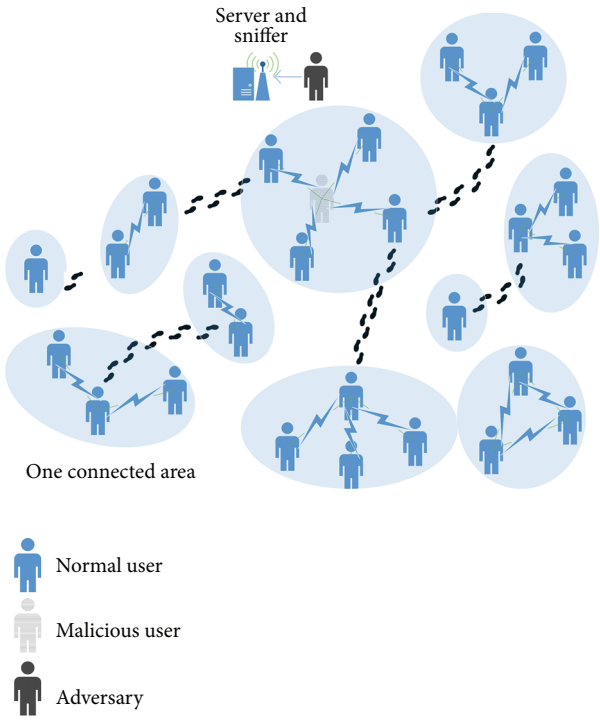

Figure 3: Threat model of the working people application scenario.

(i) *PEKS*: it inputs public key of some node A and a keyword w, outputs a searchable encrypted keyword w', w' cannot be obtained only with w:

$$w' = PEKS\left(A_{\text{pub}}, w\right). \tag{1}$$

(ii) *Trapdoor*: it inputs private key of some node A and a keyword w and outputs the trapdoor TD_w of w. TD_w is private because computation of it needs private key:

$$TD_w = Trapdoor\left(A_{\text{priv}}, w\right). \tag{2}$$

(iii) *Test*: it inputs a searchable encrypted keyword w' and a trapdoor D, outputs *true* if and only if TD is the trapdoor of w, otherwise outputs *false*:

$$Flag = Test\left(w', TD\right). \tag{3}$$

(2) *CP-ABE* will be used in the confidentiality preserving scheme to realize a fine-grained access control strategy. It consists of four preliminaries: *CPA_Setup*, *CPA_Encrypt*, *CPA_KeyGen,* and *CPA_Decrypt*.

(i) *CPA_Setup*: setup of *CP_ABE* needs a third party authority. Firstly let G_1 be a bilinear group of prime order p, and let g be a generator of G_1. Secondly choose two random components $\alpha, \beta \in Z_p$ and then publish the public key and master key:

$$CPA_{\text{pub}} = \left\{G_1, g, h = g^{\beta}, f = g^{1/\beta}, e(g,g)^{\alpha}\right\}, \tag{4}$$
$$CPA_{\text{master}} = \left\{\beta, g^{\alpha}\right\}.$$

(ii) *CPA_Encrypt*: sender makes the access policy T_M for the message about to be sent, encrypts plain text M, and gets cipher text CT:

$$CT = CPA\_Encrypt\left(CPA_{\text{pub}}, M, T_M\right). \tag{5}$$

(iii) *CPA_KeyGen*: the receiver submits its attributes set S to authority, and authority uses CPA_{master} and S to compute the private key $CPA_{\text{priv},S}$:

$$CPA_{\text{priv},S} = CPA\_KeyGen\left(CPA_{\text{master}}, CPA_{\text{pub}}, S\right). \quad (6)$$

(iv) *CPA_Decrypt*: in the end, receiver uses $CPA_{\text{priv},S}$ to decrypt CT if S satisfies T_M, receiver will get M.

$$M = CPA\_Decrypt\left(CT, CPA_{\text{priv},S}, T_M\right). \quad (7)$$

4.2. PEFKS-Based Privacy Preserving Forwarding Scheme

(1) *Initialization*. The initialization is completed by the trusted third party TTP. It possesses a public key TTP_{pub} and a private key TTP_{priv}. It should be noticed that, TTP is not always on-line in lifetime of opportunistic network; in fact, it only works when a new user registers to participate. As for *PEFKS*, TTP will distribute its TTP_{pub} to every user registering. When a subscriber A_i submits its candidate interests set $W^*_{A_i}$ to TTP, TTP constructs a fuzzy set for every word in $W^*_{A_i}$ using dictionary-based fuzzy set construction [13]:

$$F^{D_0}_{w,d} = \left\{w', ed\left(w', w\right) \le d,\ w' \in D_0\right\}, \quad \text{for each } w \text{ in } W^*_{A_i}. \quad (8)$$

Then trusted third party (TTP) constructs trapdoor sets for all fuzzy sets using private key of TTP and returns them to A_i:

$$T_{A_i,w} = \left\{TD = Trapdoor\left(TTP_{\text{priv}}, w'\right), \text{for each } w' \text{ in } F^{D_0}_{w,d}\right\}. \quad (9)$$

After the registration, TTP can be off-line for some time. There may be a doubt why TTP cannot always be on-line to process the subscriber's changing interests. The reason is simple; in opportunistic network, stable connections cannot be guaranteed, nor a centric security service.

(2) *Construction of Forwarding Tables*. If one subscriber A_i wants to broadcast its interest advertisement, it chooses the necessary trapdoor sets from all candidate ones obtained when registering, then uses the trapdoor sets as new CI_{A_i}, and broadcasts new RA_i to all intermediate nodes it meets. After intermediate node B_k receives RA_i, it will create a new record in its forwarding table composed of two parts; the first part is CI_{A_i} of RA_i and the second is the identity of A_i. The process is described in Figure 4.

When intermediate B meets D, it firstly does the lookup of FT_B and delivers messages in $List_B$. Then it fetches all records from its FT_B, adds self-identity to the second part of every forwarding table record, and exchanges it with D.

(3) *Secure Lookup of Forwarding Tables*. When publisher C_j has new payload P_{C_j} to publish, it chooses keywords that can index the payload to form a set $W_{C_j} = \{w_{C_j,1}, w_{C_j,2}, \ldots, w_{C_j,M_{C_j}}\}$ and then encrypts them based on *PEKS* to get a set of searchable encrypted keywords which will be used as new CI_{C_j}:

$$PEKS_{C_j} = \left\{w' = PEKS\left(TTP_{\text{pub}}, w\right), \text{ for each } w \text{ in } W_{C_j}\right\}. \quad (10)$$

With CI_{C_j}, the encrypted payload $E(P_{C_j})$ and the access policy $T_{P_{C_j}}$ together, C_j forms a new PC_j and broadcasts it to every intermediate node it meets. Details about $E(P_{C_j})$, and $T_{P_{C_j}}$ will be discussed in the following section. The process is described in Figure 5.

When intermediate node B meets some other one D, it would execute *SecureLookup* algorithm and decide whether to forward some messages to it.

In *SecureLookup* algorithm, the subfunction *FuzzyTest* function is used to calculate the similarity between S_{TD} and $S_{w'}$ (see Algorithms 1 and 2). Here S_{TD} means the control information from a record of forwarding table and $S_{w'}$ means the control information of a published content. A larger returned value means a higher similarity. If the result of *FuzzyTest* is higher than threshold, the payload will be delivered to D.

```
Foreach ft in FT_B
  If (D ∈ ft · SID) == true)
    Foreach pc in List_B
      similarity = FuzzyTEST (ft · RI, pc · CI);
      If (simlarity ≥ TH) {TH: threshold to deliver}
          deliver pc · P to D;
          break;
      End
    End
  End
End
```

Algorithm 1: *SecureLookup* (FT_B, D).

```
Define Counter = 0
Foreach td in S_TD
  Foreach w' in S_w'
    If (Test (w', td) == true) Counter ++;
    End
  End
End
Return Counter;
```

Algorithm 2: *FuzzyTest* (S_{TD}, $S_{w'}$).

4.3. CP-ABE-Based Confidentiality Preserving Scheme

(1) *Initialization*. TTP is responsible for initialization of *CP-ABE* including the creation of public key CPA_{pub} and the master key CPA_{master}. Having finished the key generation,

TTP will broadcast CPA_{pub} to every user intending to participate in the system. The registration stage also involves authentication which is beyond the scope of this paper. After the registration, a subscriber A_i submits its attributes set Y_{A_i} to the trusted third party which is responsible for calculating the corresponding private key $CPA_{\text{priv},Y_{A_i}}$ and returning it to A_i. After the registration, *TTP* could be away from the connected areas of the system:

$$CPA_{\text{priv},Y_{A_i}} = CPA\_KeyGen\left(CPA_{\text{master}}, CPA_{\text{pub}}, Y_{A_i}\right). \tag{11}$$

(2) *Encryption of Published Content*. When a publisher C_j has new contents to publish, he firstly creates an access policy in which designated subscribers' attribute requirements are described, and then he would encrypt the content with CPA_{pub} to get cipher text $E(P_{C_j})$:

$$CPA_{\text{priv},Y_{A_i}} = CPA\_KeyGen\left(CPA_{\text{master}}, CPA_{\text{pub}}, Y_{A_i}\right). \tag{12}$$

(3) *Decryption of Published Content*. The encrypted published content message is then forwarded according to some kind of content-based routing scheme which of course could be our proposed *PEFKS*-based interest-centric routing scheme. When a subscriber who is interested in the content receives the message, it tries to decrypt. If and only if the subscriber's personal attribute set satisfies the access policy, the decryption succeeds and he gets the plaintext:

$$P_{C_j} = CPA\_Decrypt\left(CT, CPA_{\text{priv},Y_{A_i}}, E\left(P_{C_j}\right)\right). \tag{13}$$

The subscheme mentioned previously is illustrated in Figure 6.

5. Evaluation and Analysis

In this chapter we will evaluate and analyze the security and the performance of our schemes.

5.1. Security. First is the security requirement of privacy. In our scheme, users' full privacy is well preserved by *PEFKS*.

PEFKS is reliable in terms of cryptography concerns, owing to deriving from *PEKS*. In [9], Boneh proved that PEKS is able to resist chosen keyword attack in random oracle model [21] in the assumption that bilinear Diffie-Hellman problem is difficult. In other words, having no trapdoors of keywords, obtaining the plain text of keyword is impossible. In our *PEFKS* utilizing, the creation process of trapdoors relies on private key of *TTP* which indicates that only *TTP* is allowed to calculate and distribute the trapdoors. To support search on encrypted fuzzy keywords, a fuzzy set related to every submitted keyword is created firstly. For every single word in a fuzzy set, the analysis is the same as in the case of PEKS [9].

Some people might have doubts about the possibility of brute force attack performed by adversary who has almost unlimited calculation power and storage space. The adversary would try generating as many encrypted keywords as possible, using the public key. In our proposed solution, fuzzy interests add a second layer of anonymity for users by blurring users' real interests. The reason is that only one keyword in a fuzzy set could reveal real interests of some users. Even if an adversary consumes huge time and space to achieve the indexes of published contents, what he actually gets is only a set of fuzzy words, which makes it very hard to acknowledge user's true privacy. Such a trick corresponds to k-anonymity protection model introduced in [22].

As for threats caused by malicious users who are already authenticated by *TTP*, they also could not work out in our proposed scheme. The most dangerous security pitfall is

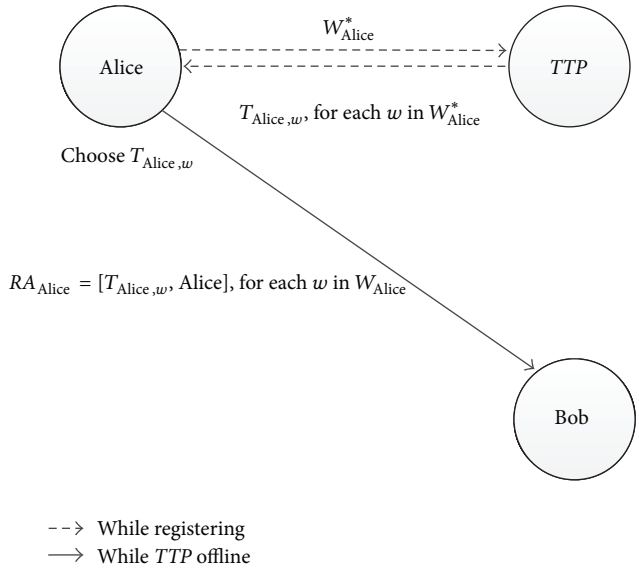

Figure 4: Setup of one record in forwarding table.

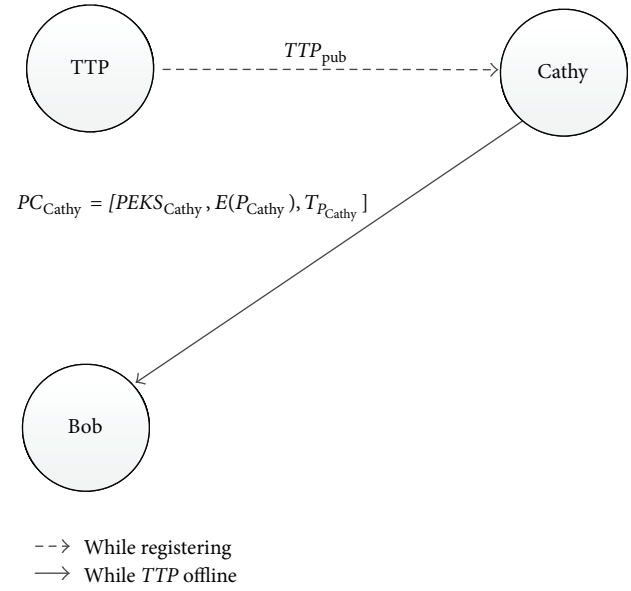

Figure 5: Create and publish new content.

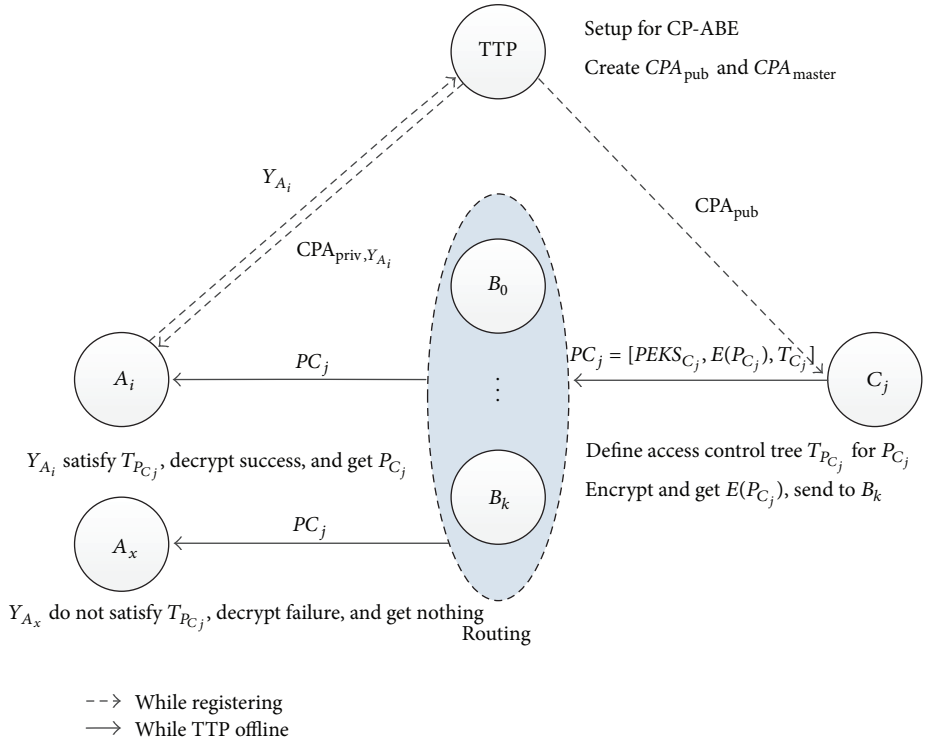

FIGURE 6: *CP-ABE*-based confidentiality protecting scheme.

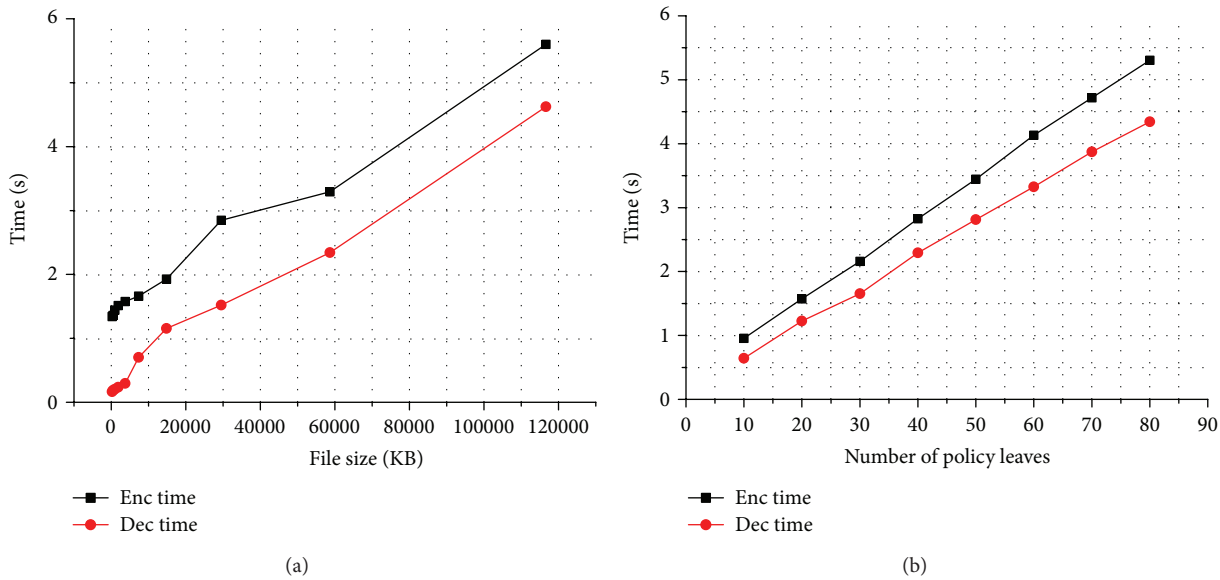

FIGURE 7: *CP-ABE* encryption and decryption time cost: (a) the x-axis corresponds to the complexity of the access policy; (b) the x-axis corresponds to the complexity of access control strategy tree.

when malicious users act as intermediate nodes, which is prevented completely in our scheme. On one hand, creation and exchange of forwarding tables involve no cryptographic operations on encrypted keywords which keeps valuable information safe. On the other hand, lookup of forwarding tables and decisions of forwarding is based on *FuzzyTest*, in which the similarity is calculated using a trapdoor set and a searchable encrypted keyword set as inputs. In all these processes, neither plaintext of interests nor relation between an interest keyword and a user is leaked. Thus full privacy presented by Shikfa et al. [1] is achieved.

Second is the confidentiality requirement. In loosely trusted environment of opportunistic network, the main challenge for confidentiality is collusion attack, which is also

Table 1: Comparison of security features.

Security feature	Nguyen et al. [4]	Symington et al. [5]	Shikfa et al. 2009 [6]	Shikfa et al. 2010 [1]	Proposed scheme
End-to-end payload encryption	Yes	Yes	Yes	Yes	Yes
Resilience to dictionary attack	No	Yes	Yes	Yes	Yes
User's full privacy	No	No	Yes	Yes	Yes
Decryption based on content/context	No	No	No	Yes	Yes
Secure partial match in forwarding	No	No	No	Yes	Yes
Secure fuzzy keyword index	No	No	No	No	Yes
Secure multiple keyword index	No	No	No	No	Yes
Secure access control strategy for message	No	No	No	No	Yes

Table 2: File size before and after encryption of *CP-ABE*.

Published content ID	File size (KB)		
	Before encryption	After encryption	Added size
1	239	241	2
2	473	475	2
3	951	953	2
4	1843	1845	2
5	3711	3713	2
6	7365	7367	2
7	14844	14846	2
8	29511	29513	2
9	58678	58680	2
10	116632	116634	2

the core challenge of *ABE*. In *CP-ABE*, *KeyGen* uses two layers of random masking to create private keys. Private key for every user is related to the second layer of random masking; thus even if two or more subscribers conclude sharing their submitted attributes and related private keys, the collusion attack will not take effect. The detailed demonstration is illustrated in [16, 19].

Comparison of security features between our proposed scheme and other aforementioned schemes in context of content-based opportunistic network is shown in Table 1. It could be seen that the proposed scheme achieves most security features of them.

5.2. Performance. The performance of *PEFKS* mainly relies on the size of the trapdoor set from a forwarding table record and the size of the searchable keyword set from a published content. Dictionary-based filter strategy used here could decrease the size of a fuzzy set dramatically, thus speeding up the calculation of *FuzzyTest* algorithm.

To evaluate the performance of *CP-ABE*, we conducted several experiments on a virtual machine equipped with Core 2 Duo based on jPBC library [23] which is a java version PBC library [24]. We measured the time required for encryption and decryption under various scenarios. Besides, we measured the cipher text size overhead incurred by our scheme to see if an acceptable cost exists in storage.

From Figure 7 we can see that the encryption and decryption time of *CP-ABE* has a significant linear correlation with the size of published content and the complexity of access policy. Considering the file size, even for a file of 120 Mbytes, it costs less than 6 seconds. Considering the complexity of access policy, encryption and decryption time for an access control strategy tree with 80 leaves is still no more than 6 seconds. In an age that mobile devices strong in computing power and storage are widespread, such a time cost is acceptable. What is more, in the application environment of opportunistic network, publishers or subscribers are not worried to encrypt or decrypt, which will leave enough time for security operations.

From Table 2. we can see that no matter what size the original published content is, the cipher text is always 2 Kbytes larger, meaning *CP-ABE* costs almost no storage redundancy in practice.

6. Conclusion

In this paper, we introduced the concept of interest-centric and attribute-based identities into opportunistic network. We focused on the security issues of user privacy and end-to-end confidentiality in a specific distributed application scenario of wireless opportunistic network, in which people work in near areas and share information without revealing their identity.

Finally, we proposed our *PEFKS*- and *CP-ABE*-based distributed security scheme which consists of two sub schemes. The first is a *PEFKS*-based privacy preserving forwarding decision scheme which assures users' full privacy and enhances anonymity through fuzzy interests. As far as we know, we are the first to employ fuzzy technique in opportunistic network and to allow partial match on encrypted fuzzy control information. The second is a *CP-ABE*-based confidentiality protecting scheme, in which publishers make and attach an expressive access control strategy to the messages they are about to send, and then subscribers whose attribute-based identities satisfy the access control strategy are legalized to decrypt cipher-text, finally achieving confidentiality with a fine-grained access control strategy on shared data. Both schemes rely on an offline *TTP* which is needed only when opportunistic network user registers.

We evaluated our scheme from aspects of security and performance, which leads to the conclusion that our scheme

suits the features of opportunistic network very well, because of not only the relatively low cost in computation and storage but also its satisfaction with necessitous need for fine-grained access control.

Acknowledgments

This paper is supported in part by Important National Science & Technology Specific Projects under Grant nos. (2010ZX03006-002, 2010ZX03006-007), National Basic Research Program of China (973 Program) (no. 2011CB302803), and National Natural Science Foundation of China (NSFC) under Grant no. (61173132, 61003307). The authors alone are responsible for the content of the paper.

References

[1] A. Shikfa, M. Önen, and R. Molva, "Privacy and confidentiality in context-based and epidemic forwarding," *Computer Communications*, vol. 33, no. 13, pp. 1493–1504, 2010.

[2] P. Hui, A. Chaintreau, R. Gass, J. Scott, J. Crowcroft, and C. Diot, "Pocket switched networking: challenges, feasibility and implementation issues," *Lecture Notes in Computer Science*, vol. 3854, pp. 1–12, 2006.

[3] L. Lilien, Z. Kamal, V. Bhuse, and A. Gupta, "Opportunistic networks: the concept and research challenges in privacy and security," in *Proceedings of the NSF International Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks*, 2006.

[4] H. A. Nguyen, S. Giordano, and A. Puiatti, "Probabilistic routing protocol for intermittently connected mobile ad hoc network∗ (PROPICMAN)," in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM '07)*, pp. 1–6, Espoo, Finland, June 2007.

[5] S. Symington, S. Farrell, H. Weiss, and P. Lovel, *Bundle Security Protocol Specification Draft-Irtf-Dtnrg-Bundle-Security-19*, 2011.

[6] A. Shikfa, M. Önen, and R. Molva, "Privacy in content-based opportunistic networks," in *Proceedings of the International Conference on Advanced Information Networking and Applications Workshops (WAINA '09)*, pp. 832–837, Bradford, UK, May 2009.

[7] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Networks*, 2011.

[8] M. Shin, C. Cornelius, D. Peebles, A. Kapadia, D. Kotz, and N. Triandopoulos, "AnonySense: a system for anonymous opportunistic sensing," *Pervasive and Mobile Computing*, vol. 7, no. 1, pp. 16–30, 2011.

[9] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," *Lecture Notes in Computer Science*, vol. 3027, pp. 506–522, 2004.

[10] S. Ji, G. Li, C. Li, and J. Feng, "Efficient interactive fuzzy keyword search," in *Proceedings of the 18th International Conference on World Wide Web*, Madrid, Spain, 2009.

[11] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in *Proceedings of the IEEE (INFOCOM '10)*, pp. 1–5, San Diego, Calif, USA, March 2010.

[12] E. S. Ristad and P. N. yianilos, "Learning string-edit distance," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 5, pp. 522–532, 1998.

[13] L. Chang, Z. Liehuang, L. Longyijia, and T. Yuran, "Fuzzy keyword search on encrypted cloud storage data with small index," in *Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS '11)*, pp. 269–273, 2011.

[14] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*, G. Blakley and D. Chaum, Eds., vol. 196, pp. 47–53, Springer, Berlin, Germany, 1985.

[15] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of the Advances in Cryptology (CRYPTO'01)*, J. Kilian, Ed., vol. 2139, pp. 213–229, Springer, Berlin, Germany, 2001.

[16] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '05)*, pp. 457–473, May 2005.

[17] J. S. Su, D. Cao, X. F. Wang, Y. P. Sun, and Q. L. Hu, "Attribute-based encryption schemes," *Journal of Software*, vol. 22, pp. 1299–1315, 2011.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, pp. 89–98, Alexandria, VA, USA, November 2006.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proceedings of the S and P IEEE Symposium on Security and Privacy (SP '07)*, pp. 321–334, Berkeley, Calif, USA, May 2007.

[20] A. Shikfa, M. Onen, and R. Molva, "Privacy-preserving content-based publish/subscribe networks," *Emerging Challenges for Security, Privacy and Trust*, vol. 297, pp. 270–282, 2009.

[21] X. Jia, B. Li, and Y. Liu, "Random oracle model," *Journal of Software*, vol. 23, pp. 140–151, 2012.

[22] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowlege-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[23] jPBC, "Java Pairing Based Cryptography," http://gas.dia.unisa.it/projects/jpbc.

[24] PBC, "Paring Based Cryptography," http://crypto.stanford.edu/pbc.