Secure Data Retrieval through Open Control in Critical Machine Network

[1]Latha.R,.[2]Sarathkumar.S
[1]Assistant Professor ,[2] PG Scholar,Department of MCA.
[1]latha@velhightech.com,[2]kumarsarath.sk@gmail.com
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala College of Engineering.

***Abstract*—Technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CPABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism too securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.**

***IndexTerms*—Access control, attribute-based encryption (ABE), disruption-tolerantnetwork (DTN), multiauthority, secure data retrieval.**

1. INTRODUCTION

In many network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments [1]–[3]. Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. Roy [4] and Chuah [5] introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced [6], [7]. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store a confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) [4], [8], [9]. We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN [10]

The concept of attribute-based encryption (ABE) [11]–[14] is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext [13]. Thus, different users are allowed to decrypt different pieces of data per the security policy.

However, the problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group). This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. IEEE TRANSACTIONS ON NETWORKING VOL:22 NO:1 YEAR 2014 If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-

grained access policies over attributes issued from different authorities. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

A. Related Work

ABE comes in two flavours called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes [4], [7], [15].

1) ***Attribute Revocation****:* Bethencourt *et al.* [13] and Boldyreva *et al.* [16] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [8], [13], [16], [17] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [18].

It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes frequently, e.g., position or location move when considering these as attributes [4], [9]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a ciphertext is encrypted with a policy that can be decrypted with a set of attributes (embedded in the user's keys) for users with. After time, say, a user newly holds the attribute set.

Even if the new user should be disallowed to decrypt the ciphertext for the time instance, he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time, he can still decrypt the ciphertext of the previous time instance unless the key of the user is expired and the ciphertext is reencrypted with the newly updated key that the user cannot obtain.

We call this uncontrolled period of time windows of vulnerability. The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the no revoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects thewhole nonrevoked users who share the attribute [19]. This could be a bottleneck for both the key authority and all nonrevoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses [4], [14]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance.

This scheme will pose overhead group elements[1] additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt *et al.* [13], where is the maximum size of revoked attributes set. Golle *et al.* [20] also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a ciphertext is exactly half of the universe size.

2) Key Escrow: Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [11], [13], [14], [21]–[23]. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase *et al.* [24] presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases and requires each user to store additional auxiliary key

1The group elements mean those in the pairing operation group, not the user group. Since the computation in ABE schemes is done in the pairing operation group , the group elements in the manuscript means group elements in the pairing group components besides the attributes keys, where is the number of authorities in the system.

3) Decentralized ABE*:* Huang *et al.* [9] and Roy *et al.* [4] Proposed decentralized CP-ABE schemes in the multiauthority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2"

OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multiencrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively. Then, the only access policy expressed with is , which can be achieved by encrypting a message with by , and then encrypting the resulting ciphertext with by (where is the ciphertext encrypted under), and then encrypting resulting ciphertext with by , and so on, until this multiencryption generates the final ciphertext . Thus, the access logic should be only AND, and they require iterative encryption operations where is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs. Chase [25] and Lewko *et al.* [10] proposed multiauthority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

B. Contribution

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets.

The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

2. NETWORK ARCHITECTURE

Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network

A. System Description and Assumptions

Fig. 1 shows the architecture of the DTN. As shown in Fig. 1, the architecture consists of the following system entities.

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users.They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system, however they would like to learn information of encrypted contents asmuch as possible.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attributebased) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users.In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol prevents them from knowingeach other's master secrets so that none of them can generatethe whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude withthe local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

B. Threat Model and Security Requirements

1) Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

2**) Collusion-resistance**: If multiple users collude, they may
be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone [11]–[13]. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user

with attributes {"Battalion 2", "Region 2"}. Theymay succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually.We do notwant these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive users' keys.

3) Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

3. PRELIMINARIES AND DEFINITION

A. Cryptographic Background

We first provide a formal definition for access structure recapitulating the definitions in [12] and [13]. Then, we will briefly review the necessary facts about the bilinear map and its security assumption.

*1) **Access Structure**:* Let be a set of parties. A collection is monotone if : If and , then . An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) of nonempty subsets of , i.e., . The sets in are called the authorized sets, and the sets not in are called the unauthorized sets. In the proposed scheme, the role of the parties is taken by the attributes. Thus, the access structure will contain the authorized sets of attributes. From now on, by an access structure, we mean a monotone access structure.

*2) **Bilinear Pairings**:* Let and be a multiplicative cyclic group of prime order . Let be a generator of . A map is said to be *bilinear* if for all and all , and *nondegenerate* if for the generator of . We say that is a bilinear group if the group operation in can be computed efficiently and there exists for which the bilinear map is efficiently computable.

*3) **BilinearDiffie–Hellman Assumption**:* Using the above notations, the Bilinear Diffie–Hellman (BDH) problem is to compute given a generator of and elements for . An equivalent formulation of the BDH problem is to compute given a generator of , and elements and in . An algorithm has advantage in solving the BDH problem for a bilinear map group , where is the security parameter (the bit length of), if . If for every polynomial-time algorithm (in the security parameter) to solve the BDH problem on , the advantage is a negligible function, then is said to satisfy the BDH assumption.

*B. **Definitions***

denotes the operation of picking an element at random and uniformly from a finite set . For a probabilistic algorithm assigns the output of to the variable . denotes a string of ones, if . A function is negligible if for every constant there exists such that for all . Let be the universe of users. Let be the central authority, and be the universe of local authorities. Let be the universe of descriptive attributes in the system. Let be the set of attributes managed by (we assume each local authority manages a disjoint set of attributes such that for). Let be a set of users that hold the attribute , which is referred to as an attribute group.

4. PROPOSED SCHEME

In this section, we provide a multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bethencourt *et al.* [13], dozens of CP-ABE schemes have been proposed [7], [21]–[23]. The subsequent CP ABE schemes are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt *et al.*'s scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt *et al.*'s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch.

A. Access Tree

*1) **Description:*** Let be a tree representing an access structure. Each nonleaf node of the tree represents a threshold gate. If is the number of children of a node and is its threshold value, then . Each leaf node of the tree is described by an attribute and a threshold value . denotes the attribute associated with the leaf node in the tree. represents the parent of the node in the tree. The children of every node are numbered from 1 to num. The function returns such a number associated with the node . The index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner.

***2) Satisfying an Access Tree**:* Let be the subtree of rooted at the node . If a set of attributes satisfies the accesstree , we denote it as . We compute recursively as follows. If is a nonleaf node, evaluate for all children of node . returns 1 iff at least children return 1. If is a leaf node, then returns 1 iff

B. Scheme Construction

Let be a bilinear group of prime order , and let be a generator of . Let denote the bilinear map. A security parameter, , will determine the size of the groups.We will also make use of Lagrange coefficients for any and a set, ,of elements in : define .Wewill additionally employ a hash function to associate each attribute with a random group element in , which we will model as a random oracle.

*1) **System Setup**:* At the initial system setup phase, the trusted initializer2 chooses a bilinear group of prime order with generator according to the security parameter. It also chooses hash functions from a family of universal one-way hash functions. The public parameter *param* is given by . For brevity, the public parameter *param* is omitted below.

5. ANALYSIS

In this section, we first analyze and compare the efficiency of the proposed scheme to the previous multiauthority CP-

ABE schemes in theoretical aspects. Then, the efficiency of the proposed scheme is demonstrated in the network simulation in terms of the communication cost. We also discuss its efficiency when implemented with specific parameters and compare these results to those obtained by the other schemes.

A. Efficiency

Table I shows the authority architecture, logic expressiveness of access structure that can be defined under different disjoint sets of attributes (managed by different authorities), key escrow, and revocation granularity of each CP-ABE scheme. In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set

TABLE
EFFICIENCY ANALYSIS

System	Ciphertext size	Rekeying message	Private key size	Public key size
BSW [13]	$(2t+1)\|G_0\|+\|G_1\|+\|G_T\|$	$l(2k+1)\|G_0\|$	$(2k+1)\|G_0\|$	$\|G_0\|+\|G_1\|$
HV [9]	$(2t+m)\|G_0\|+m\|G_1\|+\|G_T\|$	$l(2k+1)\|G_0\|$	$(2k+m)\|G_0\|$	$m\|G_0\|+m\|G_1\|$
RC [4]	$(2t+3r+m)\|G_0\|+m\|G_1\|+\|G_T\|$	0	$(3k+2m)\|G_0\|$	$n(t+4)\|G_0\|+n\|G_1\|$
Proposed	$(2t+1)\|G_0\|+\|G_1\|+\|G_T\|$	$(n-l)\log\frac{n}{n-l}\|G_p\|$	$(2k+1)\|G_0\|+\log n\|G_k\|$	$\|G_0\|+m\|G_1\|$

$|G_0|$: bit size of an element in G_0, $|G_1|$: bit size of an element in G_1, $|G_p|$: bit size of an element in Z_p^*,
$|G_k|$: bit size of a KEK, $|G_T|$: bit size of an access tree T in the ciphertext, r: the number of revoked users,
l: the number of users in an attribute group, n: the number of all users in the system,
m: the number of authorities in the system, k: the number of attributes associated with private key of a user,
n: the number of attributes in the system, t: the number of attributes appeared in T.

to the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the ciphertext. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities. Table summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update nonrevoked users' keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table II, the proposed scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its ciphertext size is linear to the number of revoked users in the system since the user revocation message is included in the ciphertext. The proposed scheme requires a user to store more KEKs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the ciphertext size while realizing more secure immediate rekeying in multiauthority systems.

B. Simulation

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [32] demonstrated the group behavior in the Internet's multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distributionwith rate , and themembership duration time follows anexponential distribution with a mean duration . Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution [32]. We suppose that user join and leave events are independently and identically distributed in each attribute group following

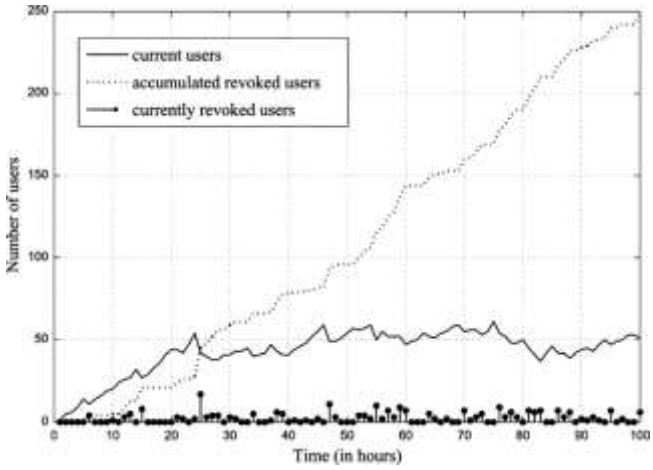
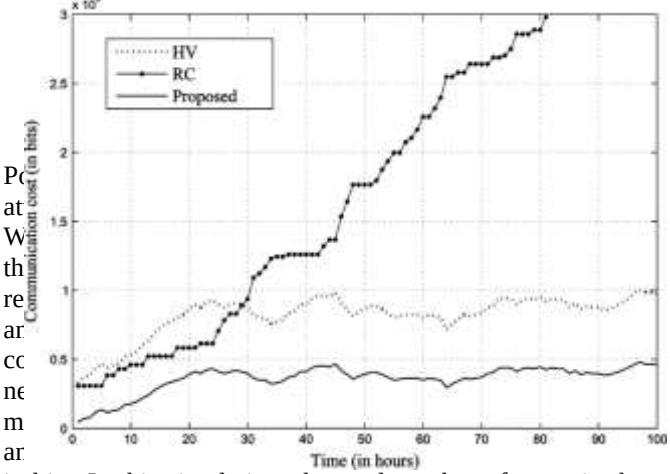


Fig. 2. Number of users in an attribute group.



Po
at
W
th
re
ar
cc
ne
m
ar
in bits. In this simulation, the total number of users in the network is

TABLE
COMPARISON OF COMPUTATION COST

		Pairing	Exp. in G_0	Exp. in G_1	Computation (ms)
Time (ms)		2.9	1.0	0.2	
BSW [13]	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$		$\log t$	$5.8k+0.2\log t$ $+2.9$
HV [9]	S		$2t+1$	1	$2t+1.2$
	U	$2k+m$		$m\log(t/m)$	$5.8k+2.9m$ $+0.2m\log(t/m)$
RC [4]	S		$3t+1$	1	$3t+1.2$
	U	$3k+m$		$m\log(t/m)$	$8.7k+2.9m$ $+0.2m\log(t/m)$
Proposed	S		$2t+1$	1	$2t+1.2$
	U	$2k+1$	k	$\log t$	$6.8k+0.2\log t$ $+2.9$

S: sender, U: user

10 000, and the number of attributes in the system is 30. The number of the key authorities is 10, and the average number of attributes associated with a user's key is 10. For a fair comparison with regard to the security perspective, we set the rekeying periods in HV as min. To achieve an 80-bit security level, we set . is not added to the simulation result because it is common in all multiauthority CP-ABE schemes. As shown in Fig. 3, the communication cost in HV is less than RC in the beginning of the simulation time (until about 30 h). However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively. The proposed scheme requires the least communication cost in the network system since the rekeying message in is comparatively less than the other multiauthority schemes.

C. Implementation

Next, we analyze and measure the computation cost for encrypting (by a sender) and decrypting (by a user) a data. Weused a Type-A curve (in the pairing-based cryptography (PBC) library [33]) providing groups in which a bilinear map is defined. Although such curves provide good computational efficiency (especially for pairing computation), the same does not hold from the point of view of the space required to represent group elements. Indeed, each element of needs 512 bits at an 80-bit security level and 1536 bits when 128-bit of security are chosen. Table III shows the computational time results. For each operation, we include a benchmark timing. Each cryptographic operation was implemented using the PBC library ver. 0.4.18 [33] on a 3.0-GHz processor PC. The public key parameterswere selected to provide 80-bit security level. The implementation uses a 160-bit elliptic curve group based on the supersingular curve over a 512-bit finite field.

The computational cost is analyzed in terms of the pairing, exponentiation operations in and . The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree. Computation costs in Table III represent the upper bound of each cost. We can see that the total computation time to encrypt data by a sender in the proposed scheme is the same as BSW, while decryption time by a user requires exponentiations in more. These exponentiation operations are to realize the fine-grained key revocation for each attribute group. Therefore, we can observe that there is a tradeoff between computational overhead and granularity of access control, which is closely related to the windows of vulnerability. However, the computation cost for encryption by a sender and decryption by a user are more efficient compared to the other multiauthority schemes.

6. SECURITY

In this section, we prove the security of our scheme with regard to the security requirements discussed in Section II.

A. Collusion Resistance

In CP-ABE, the secret sharing must be embedded into the ciphertext instead to the private keys of users. Like the previous ABE schemes [11], [13], the private keys of users are randomized with personalized random values selected by the such that they cannot be combined in the proposed scheme. In order to decrypt a ciphertext, the colluding attacker should recover . To recover this, the attacker must pair from the ciphertext and from the other colluding users' private keys for an attribute (we suppose that the attacker does not hold the attribute). However, this results in the value blinded by some random value, which is uniquely assigned to each user, even if the attribute group keys for the attributes that the user holds are still valid. This value can be blinded out if and only if the user has the enough key components to satisfy the secret sharing scheme embedded in the ciphertext. Another collusion attack scenario is the collusion between revoked users in order to obtain the valid attribute group keys for some attributes that they are not authorized to have (e.g., due to revocation). The attribute group key distribution protocol, which is complete subtree method in the proposed scheme, is secure in terms of the key indistinguishability [29]. Thus, the colluding revoked users can by no means obtain any valid attribute group keys for attributes that they are not authorized to hold. Therefore, the desired value cannot be recovered by collusion attack since the blinding value is randomized from a particularuser's private key.

Collusion among the local authorities could determine the personalized key component of some user . However, each attribute key component of the user is blinded in the local authorities' view in that they are divided by the secret , which is only known to the user and . Therefore, the colluding local authorities cannot derive the whole setof secret keys of users.

B. Data Confidentiality

In our trust model, the multiple key authorities are no longer fully trusted as well as the storage node even if they are honest. Therefore, the plain data to be stored should be kept secret from them as well as from unauthorized users. Data confidentiality on the stored data against unauthorized users can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the ciphertext, he cannot recover the desired value during the decryption process, where is a randomvalue uniquely assigned to him.On the other hand, when a user is revoked from some attribute groups that satisfy

Another attack on the stored data can be launched by the storage node and the key authorities. Since they cannot be totally trusted, confidentiality for the stored data against them is another essential security criteria for secure data retrieval inDTNs. The local authorities issue a set of attribute keys for their managing attributes to an authenticated user , which are blinded by secret information

that is distributed to the user from . They also issue the user a personalized secret key by performing the secure 2PC protocol with . As we discussed in Theorem 1, this key generation protocol discourages each party to obtain each other's master secret key and determine the secret key issued from each other. Therefore, they could not have enough information to determine the whole set of secret key of the user individually.

Even if the storage node manages the attribute group keys, it cannot decrypt any of the nodes in the access tree in the ciphertext. This is because it is only authorized to reencrypt the ciphertext with each attribute group key, but is not allowed to decrypt it (that is, any of the key components of users are not given to the node). Therefore, data confidentiality against the curious key authorities and storage node is also ensured.

7. CONCLUSION

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption tolerant networks," in *Proc. IEEE INFOCOM*, 2006, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in *Proc. Conf. File Storage Technol.*, 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc.Eurocrypt*, 2005, pp. 457–473

.[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 2006, pp. 89–98.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

[14] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 195–203.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270. [16] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

[17] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in *Proc. ACMConf. Comput. Commun. Security*, 2006, pp. 99–112.

[18] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Comput. Surv.*, vol. 35, no. 3, pp. 309–329,2003.

[19] S. Mittra, "Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288. [20] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp. 26–35.

[21] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465.

[22] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Proc. ICALP*, 2008, pp. 579–591.

[23] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*, 2009, pp. 343–352.

[24] M. Chase and S. S. M. Chow, "Improving privacy and security inmultiauthority attribute-based encryption," in *Proc. ACM Conf. Comput.Commun. Security*, 2009, pp. 121–130.

[25] M. Chase, "Multi-authority attribute based encryption," in *Proc. TCC*,2007, LNCS 4329, pp. 515–534.

[26] S. S.M. Chow, "Removing escrow from identity-based encryption," in *Proc. PKC*, 2009, LNCS 5443, pp. 256–276.

[27] M. Belenkiy, M. Chase, M. Kohlweiss, and A. Lysyanskaya, "P-signatures and noninteractive anonymous credentials," in *Proc. TCC*, 2008, LNCS 4948, pp. 356–374.

[28] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in *Proc. Crypto*, LNCS 5677, pp. 108–125.

[29] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. CRYPTO*, 2001, LNCS 2139, pp. 41–62.

[30] C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 6

