ISSN:0975-9646



# Secure Data Retrieval Using CP-ABE for Decentralized Disruption Tolerant Military Networks

C. Rajeshwar Reddy[1], N.V. Sailaja [2]

[1]*M.Tech Student (SE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

[2]*Assistant Professor (CSE), VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India*

*Abstract*—**Disruption-tolerant network (DTN) technologies are becoming successful solutions that permit remote device conveyed by officers to speak with one another and access the confidential data or secret data by exploiting outside storage nodes. This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. However, the problem of applying CP-ABE 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 to safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network .**

*Keywords*— **Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.**

## I. INTRODUCTION

The design of the current Internet service models is based on a few ass

umptions such as (a) the existence of an end to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples [1] are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another.

In the above scenarios, an end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic, predictably connectable, or periodically connected. To allow nodes to communicate with each other in these extreme networking environments [2]-[4], Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other. 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. After the connection is eventually established, the message is delivered to the destination node.

Roy [5] and Chuah [6] 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. A requirement in some security-critical applications is to design an access control system to protect the confidential data stored in the storage nodes or contents of the confidential messages routed through the network. As an example, in a battlefield DTN, a storage node may have some confidential information which should be accessed only by a member of 'Battalion 6' or a participant in 'Mission 3'. Several current solutions [7]-[9] follow the traditional cryptographic-based approach where the contents are encrypted before being stored in storage nodes, and the decryption keys are distributed only to authorized users. In such approaches, flexibility and granularity of content access control relies heavily on the underlying cryptographic primitives being used. It is hard to balance between the complexity of key management and the granularity of access control using any solutions that are based on the conventional pair wise key or group key primitives. Thus, we still need to design a scalable solution that can provide fine-grain access control. We refer to a DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN [10].

In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt. Our scheme can provide not only fine-grained access control to each content object but also more sophisticated access control antics. Ciphertext-policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive powers.

## II. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and Ciphertext-policy ABE (CP-ABE). 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 cipher texts. Especially, Ciphertext-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]. 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 cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key. However, the roles of the cipher texts 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 [5], [9], [15].

### A. 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 [13], [16], [17], [18] have two main problems.

The first problem is the security degradation in terms of the backward and forward secrecy [19]. 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 [5], [20]. 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 reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). 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). 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 nonrevoked users can update their keys. This results in the "1-affects- " problem, which means that the update of a single attribute affects the whole nonrevoked users who share the attribute [21]. This could be a bottleneck for both the key authority and all nonrevoked users.

### B. 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], [22]–[24]. 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.* [25] 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 $O(N^2)$ communication overhead on the system setup and the rekeying phases and requires each user to store $O(N^2)$additional auxiliary key components besides the attributes keys, where N is the number of authorities in the system.

### C. Decentralized ABE

Junbeom Hur [26] and Roy *et al.* [5] proposed decentralized CP-ABE schemes in the multi authority 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 multi encrypting approaches can by no means express any general "*n*-out-of-*m*" logics (e.g., OR, that is 1-out-of- m).

## III. CP-ABE Scheme for DTNs

In this paper, we implement 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 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.

### A. Advantages

*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.

*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 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.

### B. Challenges

The problem of applying CP-ABE in decentralized disruption tolerant networks introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

## IV. DTN Architecture

In this section, we describe the DTN architecture and define the security model.

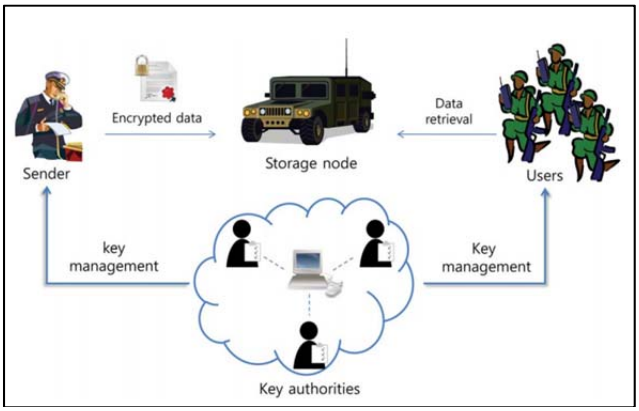


Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network.

### 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 as much 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 [5], [6]. Similar to the previous schemes, we also assume the storage node to be semi-trusted, 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 (attribute based) 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 knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

## V. Implementation

We have used Java programming language to implement the CP-ABE for DTN. In the remainder of this section, first we will discuss the proposed Disruption Tolerant military network then we combine our CP-ABE scheme with decentralized DTN for secure data retrieval.

First we have designed the Disruption Tolerant Network (DTN) which introduces the concept of storage nodes wherein the confidential data is replicated or stored such that only authorized mobile nodes can access the necessary information quickly and reliably.

The sender (commander) who owns the confidential data has the authority to register users (soldiers) and provide access privileges.

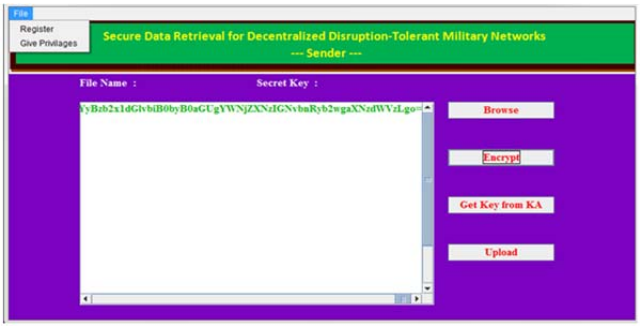


Fig. 2. Sender Module

Fig. 2 shows the sender module implementation. The confidential data is encrypted before stored in the storage node. The key Authority generates a secret key for the user with respect to the attributes set. Sender encrypts the data and defines an access policy (i.e., Combination of battalion and region) which the user needs to possess in order to decrypt the data from the storage node. The cipher text is encrypted with an access policy chosen by an encryptor and then it is stored in the storage node.


Fig. 3. Storage Node-Attackers list

Fig. 3 shows the implementation of storage node. All the files stored can be viewed in here. All users who try to access the data from the storage node without satisfying the access policy will be blocked and will be added to the attackers list.

Sender has the access to revoke any user at any point of time by unblocking them from the attackers list.


Fig. 4. Key Authority

Fig. 4 shows the functionality of key authority. The key authority generates the secret keys to the user with respect to the attribute set. It can view the list of users, list of keys given to users and the privileges assigned to different users.

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.

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 achieve this the key authorities and sender engage in a secure two party computation such that end user (soldier) needs to satisfy the access policy defined by the commander and also must have enough privileges from sender to access the confidential data.

## VI. 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 access control and to secure data retrieval issues. In this project, an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently has been implemented. 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. data.

## References

[1] M. Chuah and others. Enhanced disruption and fault tolerant network architecture for bundle delivery (EDIFY). In Proceedings of IEEE Globecom, 2005.

[2] 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.

[3] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp. as1–6.

[4] 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.

[5] S. Roy and M. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs,” Lehigh CSE Tech. Rep., 2009.

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

[7] 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.

[8] A. Harrinton and C. Jensen. Cryptographic access control in a distributed file system. In Proceedings of ACM SACMAT, 2003.

[9] 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.

[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. ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.
[18] 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.
[19] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.
[20] 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.
[21] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.
[22] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.
[23] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591
[24] 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.
[25] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.
[26] Junbeom Hur and Kyungtae Kang, Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks, IEEE/ACM transactions on networking, vol. 22, no. 1, february 2014.