International Journal of Current Research and Modern Education (IJCRME)
ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume I, Issue I, 2016

EFFICIENT TRUST ESTABLISHMENT FOR SECURE COMMUNICATION IN DELAY TOLERANT NETWORKS USING ATTRIBUTE BASED ENCRYPTION

S. Senthil Kumar* & A. Jahir Husain**
* M.Tech Scholar, PRIST University, Thanjavur, Tamilnadu
** Assistant Professor, PRIST University, Thanjavur, Tamilnadu

Abstract:

Conventional ad hoc routing protocols are not capable of work in irregularly connected networks since end-to-end paths may not exist in such networks. Hence, routing methods that can survive disruptions need to be designed. A store-and-forward approach has been proposed for delivering messages in delay tolerant networks. Delay-tolerant network (DTN) technologies are becoming successful solutions that permit wireless devices in military environments to communicate with each other and access the secret information or command reliably by exploiting external storage nodes. In this paper, we propose a protected data recovery scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We express how to apply the proposed mechanism to securely and efficiently administer the confidential data distributed in the disruption-tolerant military network.

Key Words: Delay & Disruption Tolerant Networks, Mobile Ad Hoc Networks, Cipher Text, Attribute-Based Encryption & Multi-Authority (ABE)

1. Introduction:

There are some extreme networking environments like military operations, where connections of wireless devices carried by armed forces may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in destructive atmospheres. Delay tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these types of networks [1]–[3]. Typically, if the end-to-end connection between a source and a destination pair is absent, the messages from the source node may have to wait in the middle nodes for a significant amount of time until the connection set up. In DTNs, the messages, sent over an existing link are buffered at the next hop until the next link in the path is connected. (e.g., a new node comes into the range or an existing node becomes live). This kind of message transmission process is usually referred to as the "store-carry-and-forward" approach. In this approach the routing is determined in an "opportunistic" fashion [4], [5], [6], [7].

In DTNs, packets may be dropped by an intermediate node even when it has the capability such as sufficient buffers and meeting opportunities to forward the data [4]. Routing misbehavior is done by selfish nodes that try to obtain their maximum benefit by adopting the services offered by DTN while refusing to forward the data packet from other sources.

Sometimes malicious nodes in the path launch an attack by dropping the original packets or modifying the packets. Researches done on DTN show that routing misbehavior will considerably diminish the packet delivery rate and, thus, pose a serious threat against the network performance of DTN [6] [8]. Therefore, there should be a protocol which can detect the misbehavior nodes to assure the protected DTN routing as well as the establishment of the trust Among DTN nodes.

A numerous research has been done to analyze the problem of routing misbehavior in the conventional mobile ad hoc networks. In most of the proposed solutions, neighbor node watching or destination acknowledgement mechanism is used to detect packet dropping [7]. Credit-based and reputation-based motivation methods are employed to stimulate rational nodes or revocation schemes to revoke malicious nodes [4], [8]. The existing misbehavior detection schemes are well suited for the traditional wireless networks. However the unique network characteristics of the DTN including lack of redundant path, rapid deviations in network conditions, makes it difficult to predict mobility patterns. In addition to this long feedback delay have made the neighborhood monitoring based misbehavior detection scheme incompatible for DTNs [4].

The idea of attribute-based encryption (ABE) [16]–[19] is a hopeful approach that completes the necessities for secure data recovery in DTNs. ABE features a method that facilitates an access control over encrypted data using access policies and recognized attributes among private keys and cipher texts. Particularly, cipher text-policy ABE (CP-ABE) offers a scalable method of encrypting data such that the encryptor describes the set of attributes that the decryptor requests to possess in order to decrypt the cipher text [18]. Thus, different users are allowed to decrypt diverse pieces of data per the security policy.

2. Literature Review:

Three different types of forwarding schemes have been proposed for DTNs. In the first category W. Zhao et al., 2004; W. Zhao et al., 2005, have proposed to use message ferries to collect data from stationary sources and deliver them to their destinations[9][10] For example in [10] W. Zhao et al. 2005, the authors assume that traffic demand between two nodes can be predictable. Then, they design routes for multiple ferries which can be used to minimize the average data delivery latency. They also think of how nodes can be allocated to ferries based on different assumptions about ferry interactions. However, in military operations, sometimes traffic demands between nodes cannot be easily estimated due to the alterations in battlefield situations.

In the second type the authors A. Lindgren et al., 2003; J. Burgess et al., 2006, [11][12] suggest a history-based routing method where every node retains a utility value for every other node in the network, based on a timer indicating the time elapsed since the two nodes last encountered each other. For example in [11] the authors proposed metric called delivery predictability at every node for each known destination. This metric indicates the expected amount a node will be able to deliver a message to each destination. The delivery predictability ages with time and also has a transitive property.

In the third type Y. Wang et al., 2005; S. Jain et al.2005,[13][14] have proposed a 2-hop relay forwarding scheme where the source sends multiple copies to different relaying nodes and the relaying nodes will deliver the copies available with them to the destination node when they come across the destination node. Even though such strategy will accomplish small transmission overhead, it will not support high delivery ratio for messages with short deadlines.

In [15] Haojin Zhu et al proposed, a probabilistic misbehavior detection method, for secure routing of DTN on the way to efficient trust establishment. The fundamental concept is to set up a periodically available Trusted Authority (TA) to estimate the node's behavior based on the routing evidences collected, and probabilistically checking.

.

3. System Model:

In this paper, we propose an attribute-based secure data recovery scheme using CP-ABE for decentralized DTNs. The objectives of the proposed scheme are as follows. First, immediate attribute revocation improve the backward/forward secrecy of secret data by decreasing the windows of vulnerability. Second, encryptions can be defined by a fine-grained access policy using any monotone access structure under attributes specified from any selected group of authorities. Third, the key escrow problem is resolved by an escrow-free key providing protocol that makes use of the characteristic of the decentralized DTN architecture.

The key providing protocol creates and issues user secret keys by executing a secure two-party computation (2PC) protocol.

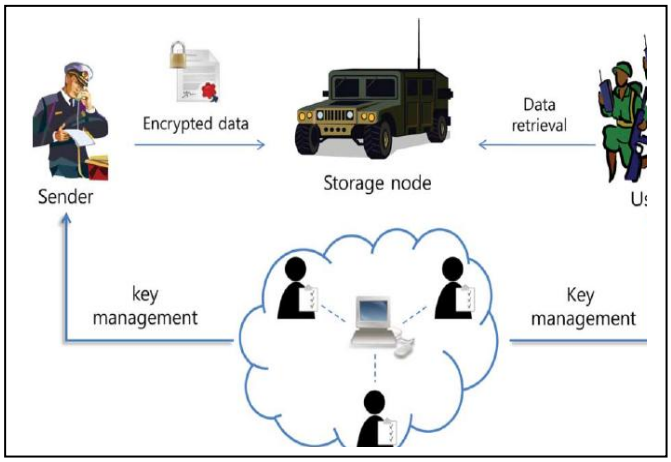

Figure 1: Secure data transmission in a disruption-tolerant military network.

3.1. Network Architecture:

In this section, we illustrate the DTN architecture with the security model.

A. System Description and Assumption.

Figure 1, Shows the architecture of the DTN. The architecture consists of the following elements:

Key Authorities: Key generation centers that generate public/secret parameters for CP-ABE. The key authorities include a central authority and multiple local authorities. It is assumed that there are protected and trustworthy communication channels between a central authority and each local authority during the initial key generation key sharing step. Each local authority administers different attributes and issues corresponding keys to users. They grant various access rights to individual users based on the users' attributes. It assumed that the key authorities will honestly execute the assigned tasks in the system.

Storage Node: This component is used to store the data from senders and give access to users. It may either be mobile or static.

Sender: The original data owner having confidential messages or data (e.g., a commander) and wishes to store them into the outside data storage node for ease of sharing or for reliable delivery to users. A sender is responsible for defining access policies and implement it on its own data by encrypting the data under the policy before storing it to the storage node.

User: A mobile node, who wish to access the data stored at the storage node (e.g., a soldier). If a user owns a set of attributes fulfilling the access policy of the encrypted data defined by the sender, then he will be able to decrypt the cipher text and obtain the data.

B. Threat Model and Security Requirements:

First of all, we assume that each node's goal is to maximize its own profit. In this work, two important kinds of DTN nodes are considered: One is the selfish node and the other is the malicious node. Due to the constraints of the resources, nodes become selfish in nature and selfish nodes are not willing to forward data packets for other nodes without sufficient reward. But a malicious node intentionally drops other nodes packet to impose an attack. The following are parameters are considered for security requirements.

Data Confidentiality: Unauthorized users who do not have enough credentials should not be allowed to access the plain data in the storage node.

Collusion-Resistance: If multiple users collude, they may be able to decrypt a cipher text by combining their keys even if each of the users cannot decrypt the cipher text separately. [16]–[18]. For example, suppose there exists a user with attributes {"Battalion 1", Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may achieve in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually.

Backward and Forward Secrecy: In the context of ABE, backward secrecy means that any user who is having an attribute (that satisfies the access policy) should be prohibited 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 lost an attribute should not be allowed from accessing the plaintext of the later data exchanged after he missed the attribute.

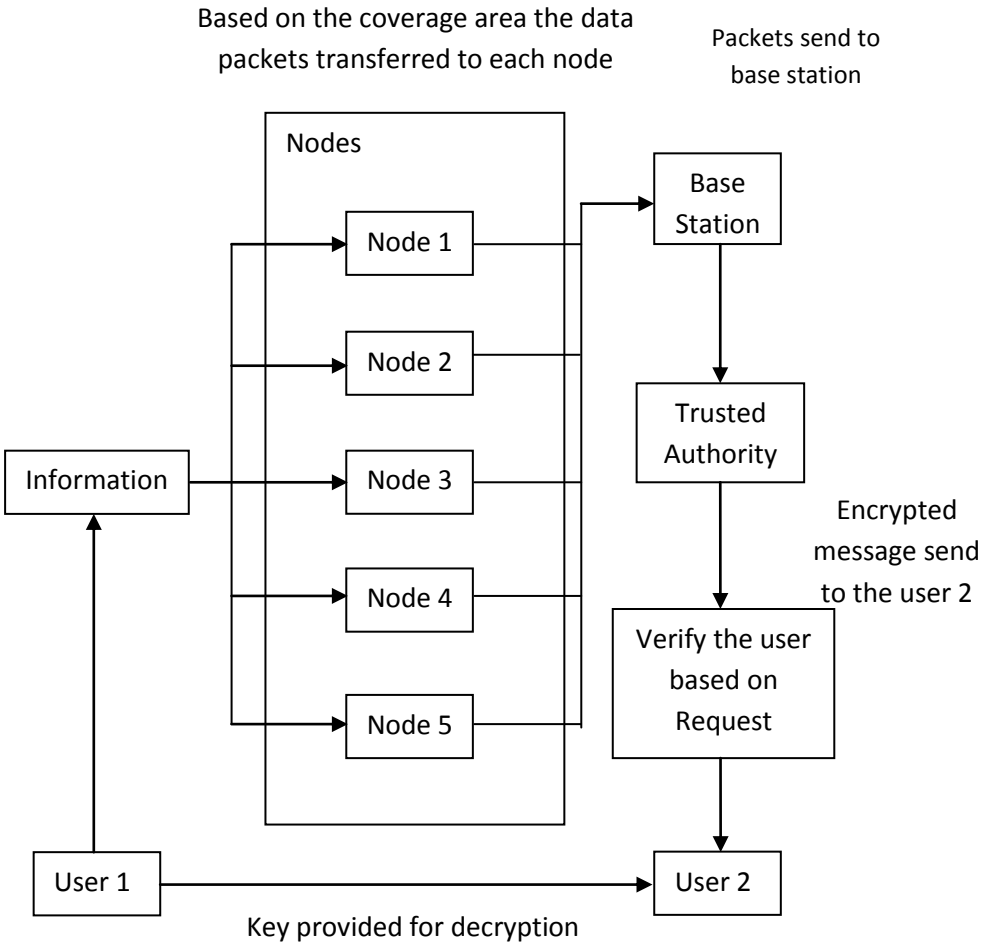

Figure 2: System Architecture

This condition is called as black hole or gray hole attack, which often happens outside of the others nodes surveillance in a sparse DTN, leading to a cruel performance degradation. This kind of the selfish behavior become complicated one by the collusion of two or more nodes.

4. Proposed Scheme:

We provide a multi authority CP-ABE method for secure data recovery in decentralized DTNs. Each local authority provides partial personalized and attribute key elements to a user by executing secure 2PC protocol with the central authority. All attribute key of a user will be updated individually and immediately. Thus, the scalability and security can be improved in the proposed scheme. Fig.2 shows the system architecture of the proposed scheme.

Since the first CP-ABE scheme proposed by Bethencourt *et al.* [18], Many number of CP-ABE schemes have been proposed [20]–[23]. The following CP-ABE schemes are mostly motivated by more accurate security proof in the standard model. On the other hand, most of the methods unsuccessful to achieve the expressiveness of the Bethencourt *et al.*'s scheme, which illustrate an professional system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Thus, in this section, we develop a variant of the CP-ABE algorithm partially based on (but not limited to) Bethencourt *et al.*'s structure so as to enhance the expressiveness of the access control policy instead of building a new CP-ABE method from scratch.

4.1. Scheme Construction:

Let G_0 be a bilinear group of prime order p , and let g be a generator of G_0. Let e: G_0 X G_0 =G_1 denote the bilinear map. A security parameter K, will determine the size of the groups. We will also make use of Lagrange coefficients $\Delta_{i,A}$ for any $i \in Z_p^*$ and a set, A , of elements in Z_p^* :

Define $\Delta_{i,A}(x) = \prod_{j \in \Lambda, j \neq i} \frac{x-j}{i-j}$ (1)

We will additionally employ a hash function H= $\{0,1\}^* \rightarrow G_0$ to associate each attribute with a random group element in G_0 , which we will model as a random oracle.

System Setup: Initially, in the system setup phase, the trusted initialize selects a bilinear group G_0 of prime order p with generator g according to the security parameter. It also selects the hash functions H= $\{0,1\}^* \rightarrow G_0$ from a family of universal one-way hash functions. The public parameter *param* is given by(G_0, g,H)

Key Generation: In CP-ABE, the elements of user secret key include a single personalized key and multiple attribute keys. The personalized key is uniquely defined for each user to prevent collusion attack among users with different attributes.

Data Encryption: When a sender wants to send its secret data M, he defines the tree access structure T over the universe of attributes L, encrypts the data under T to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm decides a polynomial q_x for every node in the tree T. These polynomials are selected in a top down manner, starting from the root node R.

Data Decryption: When a user receives the cipher text CT from the storage node, the user decrypts the cipher text with its secret key. The algorithm executes in a recursive way. We first define a recursive algorithm *Decrypt Node (CT,SK,x)* that takes the cipher text CT as input, a private key SK, which is associated with a set of attributes, and a node x from the tree T. It outputs a group element of G.

4.2. Analysis:

In this part, we first examine and compare the efficiency of the proposed method to the previous multi authority CP-ABE schemes in theoretical aspect. Then, the efficiency of the proposed scheme is established in the network simulation in terms of the communication cost.

Table I illustrates 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. The revocation in the proposed method can be done in an immediate way as contrasting to BSW. Therefore, attributes of users can be cancelled at any time even before the expiration time that might be set to the attribute. This improves the security of the stored data by minimizing the chances for misbehavior.

Table I: Expressiveness, Key Escrow, And Revocation Analysis

Scheme	Authority	Expressiveness	Key Escrow	Revocation
BSW	Single	-	Yes	Periodic attribute revocation
HV	Multiple	AND	Yes	Periodic attribute revocation
RC	Multiple	AND	Yes	Immediate system-level user revocation
Proposed	Multiple	Any monotone access structure	No	Immediate attribute level user revocation

Besides, the proposed scheme understands more fine-grained user revocation for each attribute rather than for the entire system as opposed to RC. As a result, suppose a user approaches 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 cipher text.

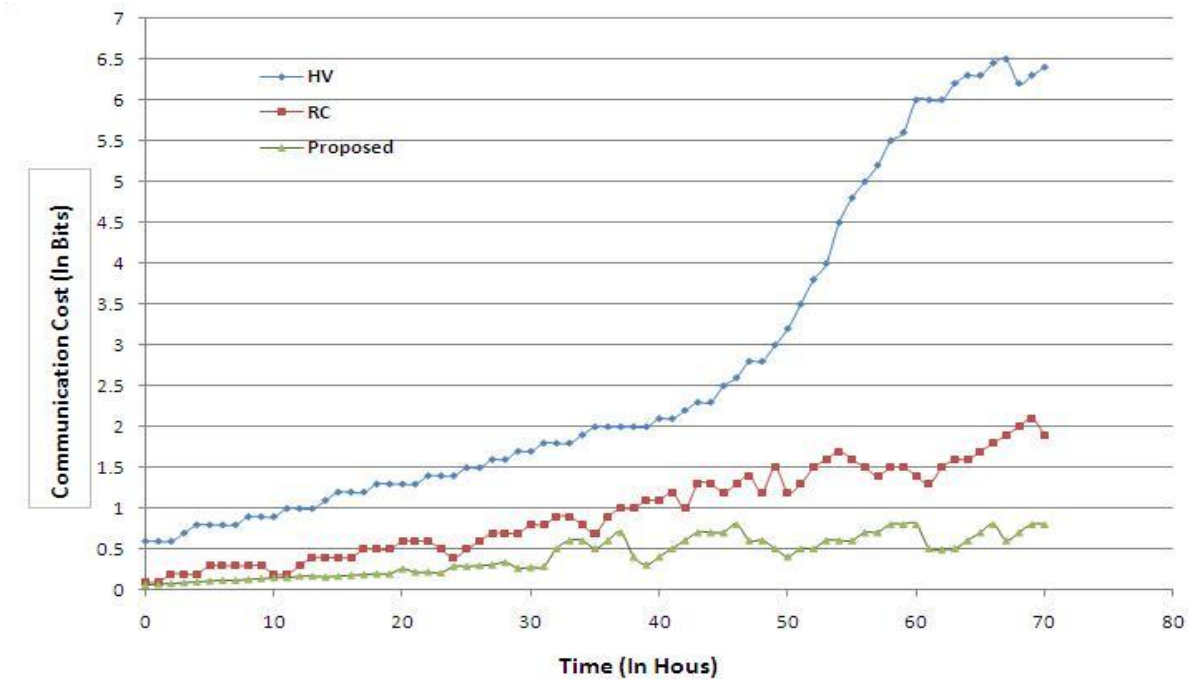

Figure 3: Communication cost in the CP-ABE systems.

Figure 3 demonstrates the total communication cost that the sender or the storage node requests to send on a membership change in each CP-ABE scheme. It comprises the cipher text and rekeying messages for non-revoked users. It is measured

in bits. For the simulation, the following parameters are used: Total number of users is 10000, 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.

5. Conclusion and Future Work:

In military environment, for the secure communication DTN technologies are becoming successful solution, since in DTN wireless devices are permitted to communicate with each other and the nodes are capable of accessing the confidential information reliably by the use of external storage nodes. CP-ABE is a scalable cryptographic method to the access control and secure data recovery problems. In this paper, we presented an efficient and secure data recovery scheme using CP-ABE for decentralized DTNs in which multiple key authorities control their attributes independently. Further, the fine-grained key revocation can be done for each attribute group. We illustrated how to utilize the proposed mechanism to make the safe, secure and efficient communication of the confidential data distributed in the disruption-tolerant military network. In future we try to implement a more secured communication for MANET and Peer to Peer to networks.

6. 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. T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.
5. Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay- Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.
6. H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.
7. H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.
8. Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.
9. W. Zhao, M. Ammar, and E. Zegura, "A message ferrying approach for data delivery in sparse mobile ad hoc networks", ACM Mobihoc, May 2004.
10. W. Zhao, M. Ammar, and E. Zegura, "Controlling the mobility of multiple data transport ferries in a Delay- Tolerant Network", Proceedings of IEEE Infocom, April, 2005.
11. Lindgren, A. Doria, O. Schelen, "Probabilistic routing in intermittently connected networks", Sigmobile, Mobile Computing and Communications Review, Vol 7(3), pp 19-20, 2003.

12. J. Burgess, B. Gallagher, D. Jensen, B.N. Levine, "MaxProp: Routing for Vehicle-Based Disruption- Tolerant Networking", to appear in Proceedings of IEEE Infocom, April, 2006.
13. Y. Wang etc, "Erasure-Coding Based Routing for Opportunistic Networks", Proceedings of Sigcom WDTN workshop, 2005
14. S. Jain, M. Demmer, R. Patra, K. Fall, "Using Redundancy to cope with Failures in a Delay Tolerant Network", Proceedings of Sigcomm 2005.
15. S. Reidt, M. Srivatsa, and S. Balfe, "The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), 2009.
16. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.
17. 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.
18. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.
19. 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.
20. 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.
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.
22. 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.