International Journal Of Advanced Engineering & Innovative Technology (IJAEIT)

ISSN: 2348 7208

IMPACT FACTOR: 1.04

Multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs

Kale Vitthal Balasaheb and Prof.Shrikant Nagure

Abstract: Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) 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 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 securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Key words: Cryptographic, Multiauthority, Cipher text-policy.

1 INTRODUCTION

In many military 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 –. 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 and Chuah 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.

Mr Kale Vitthal Balasaheb, Research Scholar and;
Prof.Shrikant Nagure, Professor at RMD Sinhgad school of Engineering Warje, Pune.
Email ID: vitthalbkale@gmail.com

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).We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. The concept of attribute-based encryption (ABE) 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, 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. Thus, different users are allowed to decrypt different pieces of data per the security policy

1.1 OVERVIEW

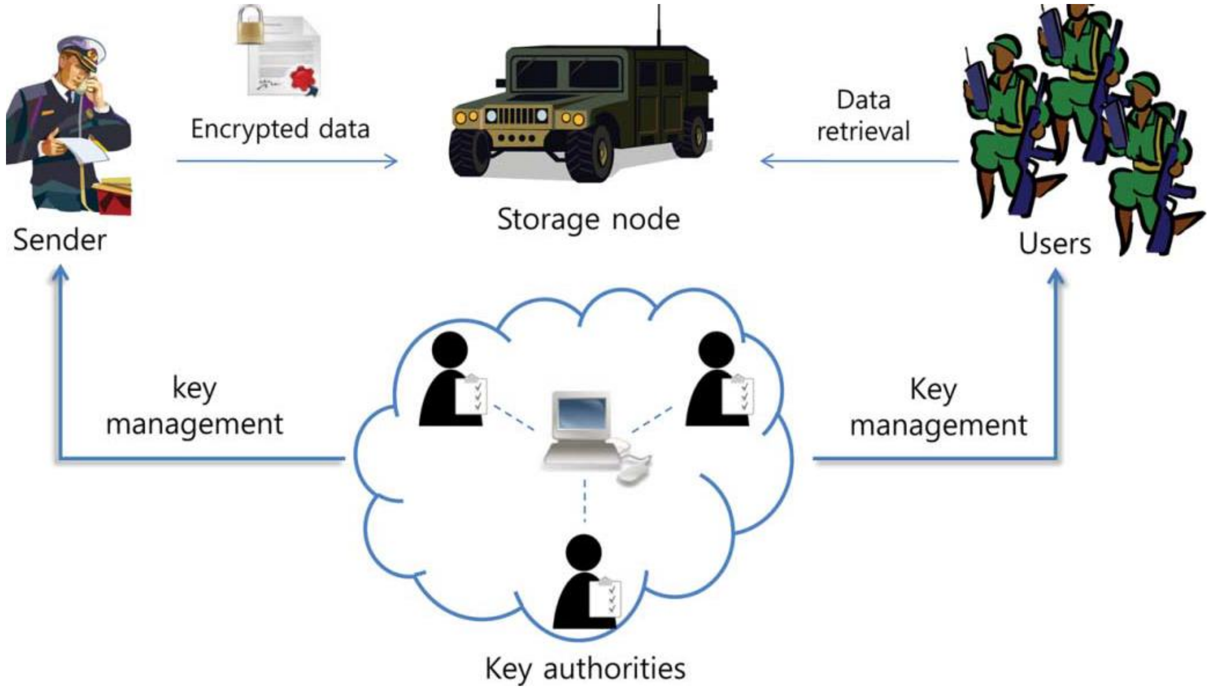

Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network.

1.2 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. 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 (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 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 withthe local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

1.3 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 –. 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.

Proposed system and Algorithm

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.* , dozens of CP-ABE schemes have been proposed . 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 access tree , 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 .We will 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.

Central Key Authority: chooses a random exponent. It set the master public/private key pair is given by.

Local Key Authorities: Each chooses a random exponent. The master public/private key pair is given by.

2) Key Generation: In CP-ABE, user secret key components consist of a single personalized key and multiple attribute keys. The personalized key is uniquely determined for each user to prevent collusion attack among users with different attributes. The proposed key generation protocol is composed of the personal key generation followed by the attribute key generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually.

Personal Key Generation: The central authority and each local authority are involved in the following protocol. For brevity, the knowledge of proofs are omitted below.

1) When authenticates a user, it selects random exponents for every local authority and sets. This value is a personalized and unique secret to the user, which should be consistent for any further attribute additions to the user. Then, and each engage in a secure 2PC protocol, where's private input is , and 's private input is . The secure 2PC protocol returns a private output to. This can be done via a general secure 2PC protocol for a simple arithmetic computation .Alternatively, we can do this more efficiently using the construction in .

2) Randomly picks then, it computes and sends it to

3) Then computes and sends it.

4) Outputs a personalized key component and sends it to the user securely. Then, the user computes its personal key component.

5.1 Advantages

1. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues.

2. It is an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently.

3. 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.

6. 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.

7. 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] 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.

[3] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in *Proc. IEEE MILCOM*, 006, pp. 1–6.

[4] L. Cheung and C. Newport, “Provably secure ciphertext policy ABE,” in *Proc. ACM Conf. Comput. Commun. Security*, 2007, pp. 456–465. V.Goyal, A. Jain,O. Pandey, andA. Sahai, “Bounded ciphertext policy attribute-based encryption,” in *Proc. ICALP*, 2008, pp. 579–591.