



Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Navnath R. Karpe, Priyanka P. Panchabuddhe, Kalyani S. Patil, Prof. V. Wande

Student, Dept. of Computer Engineering, JSPM's ICOER, Wagholi, Pune, Maharashtra, India

Student, Dept. of Computer Engineering, JSPM's ICOER, Wagholi, Pune, Maharashtra, India

Student, Dept. of Computer Engineering, JSPM's ICOER, Wagholi, Pune, Maharashtra, India

Assistant Professor, Dept. of Computer Engineering, JSPM's ICOER, Wagholi, Pune, Maharashtra, India

ABSTRACT: DTN (Disruption Tolerant Network) is successfully solution to allow the wireless devices which will be useful to soldiers to connecting each other mobile nodes in battlefield or hostile region to distress form the intermediate network connectivity and achieve secure data or some command by reliable to explore from external node. The most challenging thing in this cases are enforcement of authorized policies. Ciphertext-policy attribute-based encryption is a reliable cryptographic solution to access control problems. Hence the problem of applying (CP-ABE) Ciphertext Policy attribute based encryption for decentralized DTNs is providing many security and privacy challenges issued from different attributes. In this paper, by using CP-ABE for decentralized DTNs we define how to secure data and retrieval scheme where multiple key authorities manage their attributes independently. We described that how securely and efficiency manage the confidential data by applying proposed mechanism which is distributed in the disruption-tolerant military network.

KEYWORDS: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multi authority, secureData retrieval.

I. INTRODUCTION

Mobile In many Military network cases wireless devices connections which is followed by soldier may be disconnected temporarily by connection jam, some environment factors and mobility, mainly when they operate in hostile environments. To communicate each other in these extreme networking environments Disruption- tolerant network (DTN) technologies are solution for the allow nodes [1, 3]. When there is no any end to end connection in between source and destination pair and message from source node may wait on intermediate node for a substantial amount of time until the connection would be eventually established. In [4] and [5] author define storage nodes in DTNs where data is stored or examined that only such mobile node can access necessary information quickly and efficiently. In military applications required increased protection of confidential data with access control method that are cryptographically enforced [6], [7]. Many of the cases it is desirable to provide different access service like data access policies are define over the user's attributes and roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, on the storage node commander may store confidential data which is access by "Battalion A" who are participating in "Region B." We studies on DNA architecture for handle multiple issues and independently manage own attribute keys as DTN [10]. The attributes based encryption is promising approach which is fulfill the requirement of secure data in DTNs. ABE features a by using access policies it is mechanism of enable access control over the encrypted data and ascribed attributes among private keys and ciphertexts. One of the important thing is ciphertexts-policy ABE (CP-ABE) provided easier way of encryptor data such that the encryptor can described the attribute keys that to be need process by descriptor and convert into ciphertext [13]. However the user can decrypt the data on different way for security purpose. Hence, the problem of applying the ABE to DTNs introduces several security and privacy challenges.

At some point some users may change their associate attributes like user change the region or some private keys might be compromised, to make system secure key updating for each attribute is necessary. However, this issue is even



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

more difficult, especially in ABE systems, since each attributes shared by each user as we study multiple groups of users as attribute groups.

This defines that revocation of attributes or any single user of attribute group can effect on other users in group. Another challenge is the key escrow problem. In CP-ABE, generate private key for user by key authorities by applying the authority's master keys to user associated set of attributes. Thus, by creating attribute key, specific user can using key attribute decrypt every cipher text. Key attributes when compromised by adversaries this would be potentially threat to the data security or privacy especially when the data is highly sensitive.

The each key authority having complete privilege for create own attribute with own master secrets, the key escrow is an inherent problem in multiple authority system. A key generation method is based on signal master key and it is the basic method asymmetric encryption system as the attribute based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

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.

II. LITERATURE SURVEY

Key policy and cipher text policy is types of ABE. In KP-ABE, with the set of attribute encryptor get a label to cipher text. 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 encryptor 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], and [15].

A. Attribute Revocation

At IN [13] and [14] author define key revocation mechanism in CP-ABE and KP-ABE. 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] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy. 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 [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 re 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 re encrypted 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 re encrypted 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 the whole non revoked users who share the attribute. This could be a bottleneck for both the key authority and all no revoked 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 elements¹ additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme where is the maximum size of revoked



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

attributes set. Author 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.

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]. 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. Author presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority 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 components besides the attributes keys, where is the number of authorities in the system.

C. Decentralized ABE

In [9] and [4] 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 "-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 multi encryption 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 and in [10] author proposed multi authority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

III. PROPOSED SYSTEM

In this paper, we define CP-ABE for decentralized DTNs. we propose an attribute base secure data retrieval scheme. The following archives of our proposed system First, immediate attribute revocation enhance backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryption 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.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

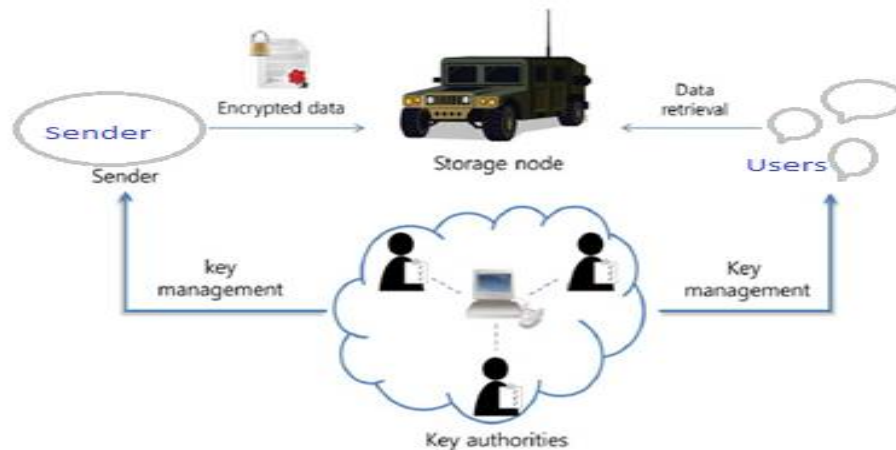


Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network.

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 In this section, we provide a multi authority 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 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 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) construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE Scheme from scratch

IV. EXPERIMENTAL RESULT

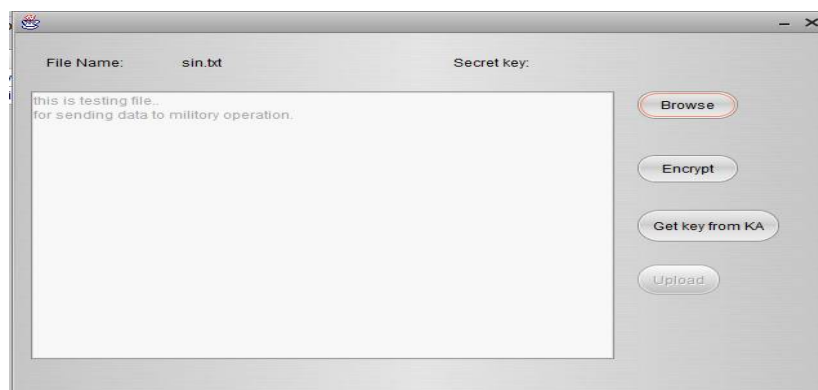


Fig 2. File select to send

Select the file and Send to the commanders.

To encrypt the particular file commander need to provide his credentials known as attributes. After getting proper attribute set then only he get the access to the file send or encrypt. The encryption of message is shows in the following figure.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

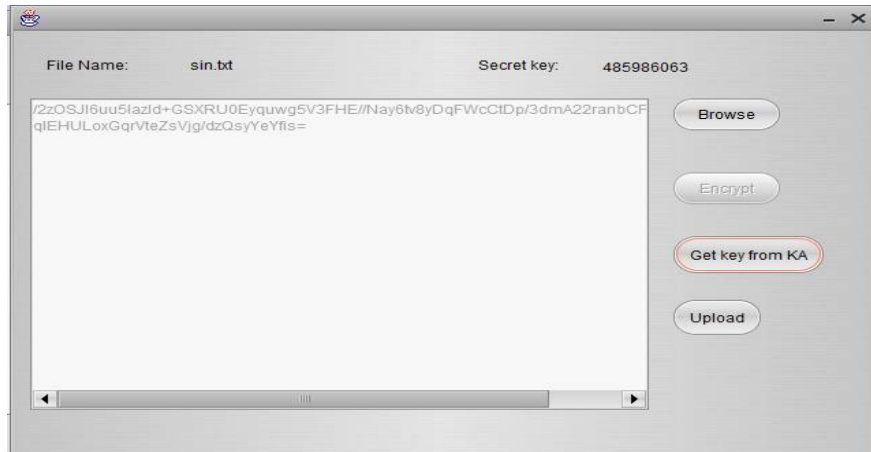
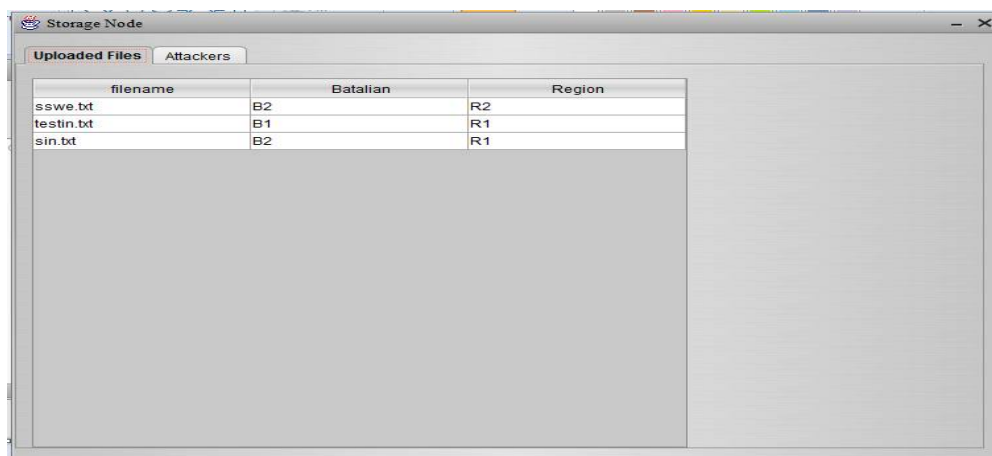


Fig 3. Access Secret Key

Access key from key access authority.

Following figure shows the storage node details. The storage node contains the files which are not delivered to the commander. Once file get delivered to the commander then file will get deleted from the storage node.



filename	Batalian	Region
sswe.txt	B2	R2
testin.txt	B1	R1
sin.txt	B2	R1

Fig. 4 storage node

V. CONCLUSION AND FUTURE WORK

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.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

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, "Message ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2006, pp. 37–48.
- [4] 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.
- [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.