Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

[#1] B.V.Koteswararao, [*2] B.Ramya Asalatha , [#3] Sk. Subhani

[1] *M Tech Student, Computer Science, Narasaraopet Engineering College, Narasaraopet, Guntur Dist, Andhra Pradesh, INDIA.*

[2,3] *Assistant Professor, CSE, Narasaraopet Engineering College, Narasaraopet, Guntur Dist, Andhra Pradesh, INDIA.*

[1] koteswararaobv@gmail.com

[2] ramyaashalatha@gmail.com

[3] shaiksubhani0338163@gmail.com

***Abstract*—Mobile nodes in military networks 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. Cipher text-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 se-cure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed distributed in the disruption-tolerant military network.**

Index Terms—Access control, attribute-based encryption (ABE) disruption-tolerant network (DTN), multi authority, secure data retrieval.

I. INTRODUCTION:

In many military network scenarios, connections of wire-less 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 mo-bile 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. 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 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 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 fulfills the requirements for se-cure 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, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encrypt or defines the attribute set that the decrypt or needs to possess in order to de-crypt the cipher text. 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 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 at-tribute 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 ex-ample, 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.

II. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE ,the encryptor only gets to label a cipher text 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 cipher text 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

a). Attribute Revocation:

Bethencourt et al and Boldyrevaet al. 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 have two main problems.

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 Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time.

c). Chase et al: 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 $O(N^2)$ 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

d). Decentralized ABE: Huang et al. and Roy et al. 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 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

Contribution

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The pro-posed 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 re-solved 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 per-forming 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 crypto-graphically enforced against any curious key authorities or data storage nodes in the proposed scheme.

III. Network Architecture

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

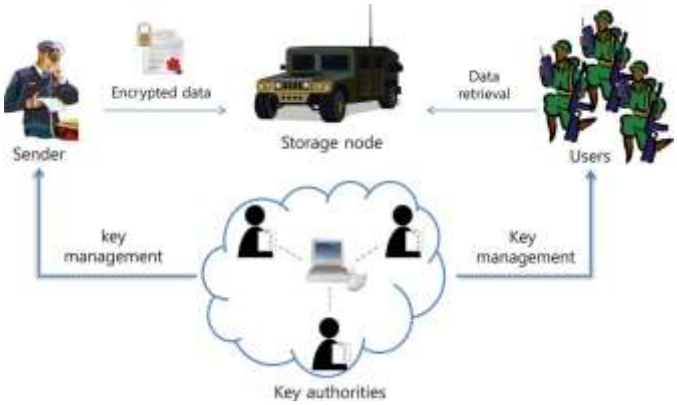

Fig. 1.Architecture of secure data retrieval in a disruption-tolerant military network.

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. 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 cipher text and obtain the data.

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 cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone. For example, suppose there exist a user

With attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed 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. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusionattack 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.

IV. PROPOSED SCHEME

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

A. Scheme Construction

In terms of the computation cost, each local authority is required to perform two more exponentiation operations. Each user needs to perform m+1multiplication operations for the key generation, which incurs negligible computation cost compared to the other pairing or exponentiation operations.

These costs would be also incurred only for the initial key generation procedures. Therefore, the additional computation overhead for the key generation using the 2PC protocol is acceptable in the system.

B. Revocation

We observed that it is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost especially in large-scaled DTNs

V. ANALYSIS

In this section, we first analyze and compare the efficiency of the proposed scheme to the previous multi authority 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 such that the access

policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV and RC 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

b).Simulation

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar demonstrated the group behavior in the Internet's multicast backbone network. They showed that the number of users joining a group follows a Poisson distribution with rate, and the membership duration time follows an exponential distribution with a mean duration1/μ. Since eachattribute group can be shown as an independent network multicastgroup where the members of the group share a commonattribute, we show the simulation result following this probabilisticbehavior distribution.

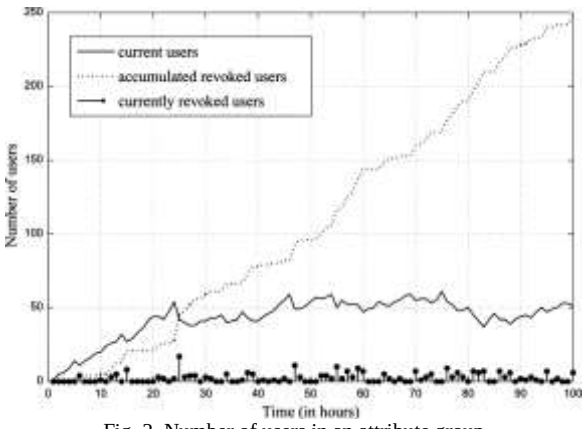

Fig. 2. Number of users in an attribute group

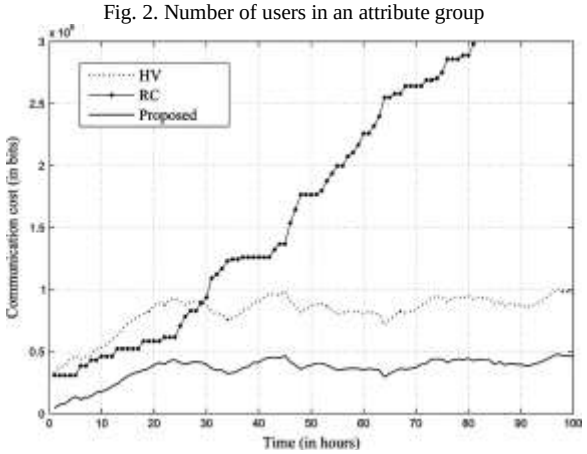

Fig. 3. Communication cost in the multiauthority CP-ABE systems.

c). Implementation

Next, we analyze and measure the computation cost for encrypting (by a sender) and decrypting (by a user) a data. We used a Type-A curve (in the pairing-based cryptography (PBC) library [33]) providing groups in which a bilinear mape:GoXG0$\rightarrow$G1is 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

VI. 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 cipher text instead to the private keys of users. Like the previous ABE schemes, the private keys of users are randomized with personalized random values selected by CA the such that they cannot be combined in the proposed scheme. In order to decrypt a cipher text, the colluding attacker should recover.

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. Even if the storage node manages the attribute group keys, it cannot decrypt any of the nodes in the access tree in the cipher text.

This is because it is only authorized to re encrypt the

cipher text 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

c). Backward and Forward Secrecy

When a user comes to hold a set of attributes that satisfy the access policy in the cipher text at some time instance, the corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key in the cipher text are re encrypted by the storage node with a random, and the cipher text components corresponding to the attributes are also re encrypted with the updated attribute group keys. Even if the user has stored the previous cipher text exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the pervious cipher text. This is because, even if he can succeed in computing from the current cipher text, it will not help to recover the desired value for the previous cipher text since it is blinded by a random. Therefore, the backward secrecy of the stored data is guaranteed in the proposed scheme.

VII. 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. ACMMobiHoc, 2006, pp. 37–48.

[4] S. Roy and M.Chuah, "Secure data retrieval based on ciphertext policyattribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-basedinformation 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, "Mediatedciphertext-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 groupbroadcast in vehicular networks using dynamic attribute based encryption,"in Proc. Ad Hoc Netw. Workshop, 2010, p. 18.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcementin 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 encryptionfor 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 attributebasedencryption," in Proc. IEEE Symp. Security Privacy, 2007, pp.321–334.

Selected Paper from International Conference on Computing (NECICC-2k15)