ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Multiauthority Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Y Katama Raju
M.Tech Student,
Department of CSE,
Loyola Institute of Technology and Management.

G.John Samuel Babu
Assistant Professor,
Department of CSE,
Loyola Institute of Technology and Management.

N.Vijay Kumar
Professor & HOD,
Department of CSE,
Loyola Institute of Technology and Management.

Abstract:

Mobile nodes in military environments such as ab-attle-field or a hostile region are likely to suffer from inter-mittent network connectivity and frequent parti-tions. Disruption-tolerant network (DTN) technologies are be-coming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or com-mand 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 encryp-tion (CP-ABE) is a promis-ing cryptographic solution to the access control issues. However, the problem of ap-plying CP-ABE in decen-tralized DTNs introduces sev-eral security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of at-tributes issued from dif-ferent authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their at-tributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disrup-tion-tolerant military network.

Index Terms:

Access control, attribute-based encryption (ABE), dis-ruption-tolerant network (DTN), multiauthority, secure data retrieval.

Introduction:

Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to com-municate with each other in these extreme net-working environments.

Typically, when there is no end-to-end connection be-tween a source and a destination pair, the messages from the source node may need to wait in the interme-diate nodes for a substantial amount of time until the connec-tion would be eventually established. In Military network scenarios, connections of wireless devices carried by sol-diers may be temporarily disconnected by jamming, en-vironmental factors, and mobility, espe-cially when they operate in hostile environments.

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 re-quire in-creased protection of confidential data includ-ing access control methods that are cryptographically enforced. In many cases, it is desirable to provide dif-ferentiated ac-cess services such that data access poli-cies 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 stor-age node, which should be accessed by members of "Bat-talion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multi-ple key authori-ties are likely to manage their own dy-namic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute represent-ing current location of moving soldiers).

It refer to this DTN architecture where mul-tiple authorities issue and manage their own attribute keys independently as a decentralized DTN. The con-cept of attribute-based encryption (ABE) is a promis-ing 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 attri-butes among private keys and ciphertexts.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryp-tor defines the attribute set that the decryptor needs to pos-sess in order to de-crypt the ciphertext. 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 se-curity and privacy challenges. Since some users may change their associated attributes at some point (for ex-ample, moving their re-gion), 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, espe-cially in ABE systems, since each at-tribute is conceiv-ably shared by multiple users (hence-forth, it refer to such a collection of users as an attribute group).

This implies that revocation of any attribute or any sin-gle user in an attribute group would affect the other us-ers 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 re-sult in bottleneck during rekeying procedure, or security degradation due to the windows of vulnerabil-ity if the previous attribute key is not updated immedi-ately. An-other challenge is the key escrow problem.

In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to us-ers' associated set of at-tributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys.If the key authority is compromised by adversaries when deployed in the hos-tile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive.

The key escrow is an inherent problem even in the mul-tiple-authority systems as long as each key author-ity has the whole privilege to generate their own attri-bute 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 asymmet-ric encryption systems such as the at-tribute-based or identity-based encryption protocols, removing escrow in single or multiple-authori-ty CP-ABE is a pivotal open problem. The last challenge is the coordination of at-tributes issued from different au-thorities.

When multiple authorities manage and issue attribute keys to users independently with their own master se-crets, it is very hard to define fine-grained access poli-cies over attributes issued from different authorities. For ex-ample, suppose that attributes "role 1" and "re-gion 1" are man-aged by the authority A, and "role 2" and "region 2" are man-aged by the authority B.

Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic be-tween attri-butes issued from different authorities can-not be imple-mented. This is due to the fact that the different authorities generate their own attribute keys using their own inde-pendent and individual master se-cret keys. Therefore, general access policies, such as "-out-of-" logic, cannot be expressed in the previous schemes, which is a very practical and commonly re-quired access policy logic.

Existing System:

•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 at-tributes among private keys and cipher-texts.

•Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryp-tor defines the attribute set that the decryptor needs to possess in order to de-crypt the ciphertext.

•Thus, different users are allowed to decrypt different pieces of data per the security policy.

•ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). 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 de-termines which ciphertexts he can decrypt and is-sues 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•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 ciphertext ad-dressed to users in the system by generating their se-cret keys at any time.

•Chase et al. presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. This approach, all (disjoint) attribute authori-ties 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.

•Disadvantages: The problem of applying the ABE to DTNs introduces several security and privacy chal-lenges. Since some users may change their associated attributes at some point (for ex-ample, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is neces-sary in order to make systems secure.

Proposed System:

•In this paper, propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independent-ly.

•It demonstrates how to apply the proposed mecha-nism to securely and efficiently manage the confiden-tial data distributed in the disruption-tolerant military network.

•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 at-tributes 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.

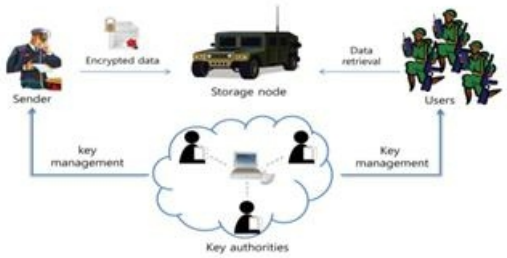
•The key issuing protocol generates and issues user secret keys by per-forming a secure two-party compu-tation (2PC) protocol among the key authorities with their own master secrets.

•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 cryptographically enforced against any curious key authori-ties or data storage nodes in the proposed scheme.

•Advantages: 1) Data Confidentiality. 2) Collusion Resistance 3) Backward and forward Secracy.

System Architecture:



Modules:

1)Key Generation

2)Multiauthority Ciphertext-policy attribute-based encryption

3)Store in Storage Node

4)Multiauthority Ciphertext-policy attribute-based decryption

Key Generation:

•Key Authorities are key generation centers that gen-erate public/secret parameters for CPABE. The key au-thorities consist of a central authority and multiple lo-cal authorities.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•It assumes that there are secure and reliable com-munication 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 us-ers 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 infor-mation of encrypted contents as much as possible.

•The user wants to access the data stored at the stor-age node, it gives the corresponding ciphertext.Multiauthority Ciphertext-Policy Attribute-Based De-cryption:

•User 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 receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key us-ing Multiauthority Ciphertext-Policy Attribute-Based Decryption.

Multiauthority Ciphertext-Policy Attribute-Based Encryption:

•Sender 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 network-ing environments.

•A sender is responsible for defining (attribute-based) access policy and enforcing it on its own data by en-crypting the data under the policy before storing it to the storage node.

•After the construction of ciphertext, the sender stores it to the storage node securely. On receiving any data request query from a user, the storage node re-sponds with to the user.

•The sender can define the access policy under attri-butes of any chosen set of multiple authorities without any restrictions on the logic expressiveness as opposed to the previous multi authority schemes.

Store in Storage Node:

•Storage node is an entity that stores data from send-ers and provide corresponding access to users.

•It may be mobile or static. Similar to the previous schemes, it also assumes the storage node to be semi trusted, that is honest-but-cu.rious.

•Then obtain the data.

CONCLUSION:

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confiden-tial 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 retriev-al method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes inde-pendently.

The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key au-thorities 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 ap-ply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disrup-tion- tolerant military network.

Refferences:

•L. Cheung and C. Newport, "Provably secure cipher-text policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

•M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473

•J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334

•S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASI-ACCS, 2010, pp. 261–270.

•A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf. Computer. Community. Security, 2008, pp. 417– 426.