

Security for Decentralized Disruption-Tolerant Military Networks

P.Bhavana

Department of Computer Science & Engineering,
GITAM University.

Yugandhar Garapati

Department of Computer Science & Engineering
GITAM University.

Abstract:

Mobile nodes in military environments such as abattlefield 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.

Index Terms:

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

Introduction:

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. In 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.

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. 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).

It 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 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 de-encrypt 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 security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), 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 attribute is conceivably shared by multiple users (henceforth, it 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 example, 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. Another 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 users' associated set of attributes. 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 hostile 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 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. The last challenge is the coordination of attributes issued from different authorities.

When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed 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 between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as "-out-of-" logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

Existing System:

- The concept of attribute-based encryption (ABE) is a promising approach that fulfills 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 de-encrypt 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 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.

- 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 addressed to users in the system by generating their secret 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 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.

- Disadvantages: 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 (for ex-ample, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary 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 independently.

- It demonstrates how to apply the proposed mechanism to securely and efficiently manage the confidential 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 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 cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

- Advantages: 1) Data Confidentiality. 2) Collusion Resistance 3) Backward and forward Secrecy.

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 generate public/secret parameters for CPABE. The key authorities consist of a central authority and multiple local authorities.

- It assumes 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.

- The user wants to access the data stored at the storage node, it gives the corresponding ciphertext. Multiauthority Ciphertext-Policy Attribute-Based Decryption:

- 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 using 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 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.

- 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 responds with to the user.

- The sender can define the access policy under attributes 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 senders 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-curious.

- Then obtain the data.

CONCLUSION:

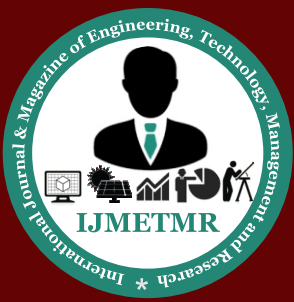
DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure 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:

- L. Cheung and C. Newport, "Provably secure ciphertext 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.



- 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.