

Secured Decentralized Confidential Data Distributed in The Disruption-Tolerant Military Network

¹Aniruddha Singh Chauhan, ²Prof. Nikita Umare

¹ME 3rd Sem. WCC Student, Abha Gaikwad-Patil College of Engineering, Nagpur, Maharashtra, India

²Dept. of CSE/WCC, Abha Gaikwad-Patil College of Engineering, Nagpur, Maharashtra, India

Abstract

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 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. We propose a secure data retrieval scheme using idea 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.

Keywords

Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN).

Introduction

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 in this extreme networking environment typically when there is no end to end connection between source and destination pairs, 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. Storage nodes in DTNs where data is stored or replicated in a way 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 and provide differentiated access service such that data access policies, which are defined as per user attributes or roles, which are managed by the key authorities.

DTN Network Architecture

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 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 entity stores data from senders and provide corresponding access to users. It may be mobile or static, we also assume the storage node to be semi trusted, that is honest-but-curious.

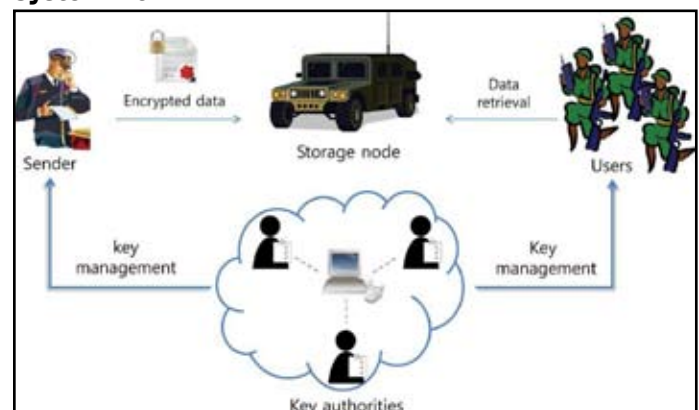
3) Sender: This entity owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible

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 mobile node 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 then he will be able to decrypt the IDEA ALGORITHM 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 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 with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

System Flow



Motivation

We provide a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. 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 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 decrypt the cipher text. 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.

The main priority to resolve following issues in proposed Project as:

1. Key Escrow
2. Decentralized ABE Scheme
3. Decentralized ABE Scheme
4. Central authority and local authority engage with MD5 Algo which prevents to know them each other master Secrets.
5. User should not revoked its attributes and satisfying access policies
6. Sender is responsible for enforcing access scheme

Problem Definition

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 [11]– [13]. For example, suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with a ttributes {"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 decryp t it individually. We do not want 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.
4. **Key Escrow:** 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 cipher text 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

Objective

1. In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic MD5 algorithm with master secret keys of their own and issue independent key components to users during the key issuing phase.
2. MD5 algorithm 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
3. We propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.
4. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture resolves the key escrow problem.
5. 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.

Methodology

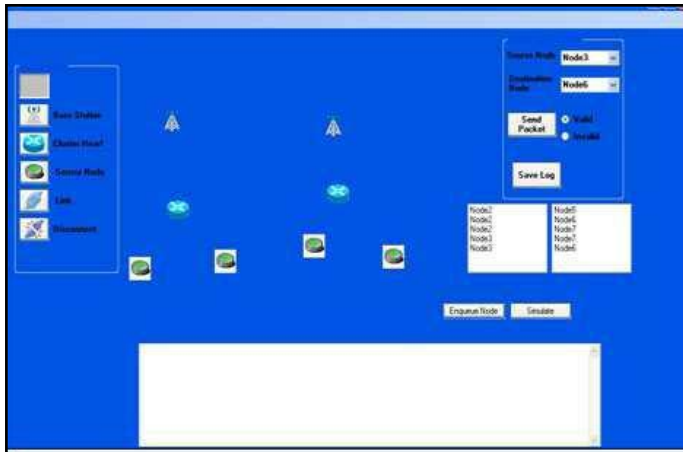
We propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors 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 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. 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.

3 DES with MD5 ALGORITHM

3DES encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It uses a 128-bit key. The algorithm consists of eight identical rounds and a "half" round final transformation. There are 2¹⁶ possible 16-bit blocks: 0000000000000000, 1111111111111111. Each operation with the set of possible 16-bit blocks is an algebraic group. Bitwise XOR is bitwise addition modulo 2, and addition modulo 216 is the usual group operation. Some spin must be put on the elements – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 (i.e., 0000000000000000) is not an element of the multiplicative

group.



Confidentiality: In order to protect sensed data and communication ex-changes between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network, case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it Does not protect against inside attacks node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information

Integrity and Authentication: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still au-thenticate themselves to the network. Hence, authentication mechanisms should be “collective” and aim at securi ng the entire network.

- In particular, the following requirements must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process:
- 1.Data aggregation is possible only if intermediate nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes that send data packets toward the base station must encrypt them with keys available to the aggregator nodes.
- 2. Data dissemination implies broadcasting of a message from the aggregator to its group members. If an aggregator shares a different key (or set of keys) with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with a different key, in order to broadcast a message to all of the nodes .But transmissions must be kept as low as possible because of their high energy consumption rate.
- **Confidentiality:** In order to protect sensed data and communication-changes between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network, case

this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station Hence ,confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information

- Integrity and Authentication: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still au-thenticate themselves to the network. Hence, authentication mechanisms should be “collective” and aim at securing the entire network.
- First, we focused on the establishment of trust relationship among wireless sensor nodes, and presented a key management protocol for sensor networks. The protocol includes support for establishing four types of keys per sensor node: individual keys shared with the base station, pairwise keys shared with individual neighboring nodes, cluster keys shared with a set of neighbors, and a group key shared with all the nodes in the network. We showed how the keys could be distributed so that the protocol can support in-network processing and efficient dissemination, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. Applying the protocol makes it hard for an adversary to disrupt the normal operation of the network.

Modules:

1. **Design of packet encryption Module:** In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. and also deploy the each port no. is authorized in a node. The intrusion detection is defined as a mechanism for a PACKET IN NETWORK to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise, the packet will be deleted. According port no only, we are going to find the path is authorized or Unauthorized. The intrusion detection is defined as a mechanism for a PACKET IN NETWORK to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized
2. **Developing software Module:** In this module, browse and select the source file .and selected data is converted into

fixed size of packets. And the packet is send from source to detector.

Conculsion

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. It 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 this method 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.

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. 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 contentbased 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 n 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, "Attributebased 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