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

Avoiding Decentralized Disruptions across Tolerant Military Networks for Security

D.Gopi
M.Tech. Student,
Dept of CSE,
Indur Institute of Engineering and Technology,
Telangana, India.

D.Parvateeswara Rao
Associate Professor,
Dept of CSE,
Indur Institute of Engineering and Technology,
Telangana , India.

ABSTRACT:

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 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:

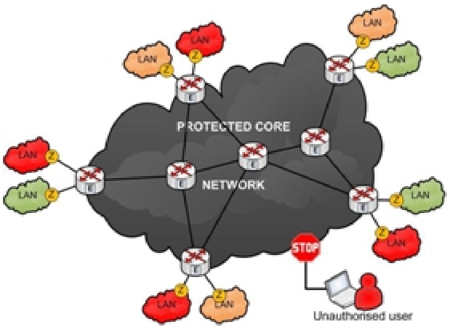
Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

INTRODUCTION:

In many 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.

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.DTN architecture may be referred as where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

By and large, it is alluring to give separated accessm administrations such that information access approaches are characterized over client qualities or parts, which are overseen by the key powers. Case in point, in an interruption tolerant military system, a commandant may store classified data at a stockpiling hub, which ought to be gotten to by parts of "Legion 1" who are partaking in "District 2." For this situation, it is a sensible supposition that numerous key powers are liable to deal with their element traits for warriors in their sent districts or echelons, which could be much of the time changed (e.g., the property speaking to current area of moving officers) [4], [8], [9]. We allude to this DTN structural engineering where various powers issue and deal with their trait keys freely as a decentralized DTN [10].



The idea of characteristic based encryption (ABE) [11]–[14] is aguaranteeing approach that satisfies the necessities for secure information recovery in DTNs. ABE characteristics an instrument that empowers a right to gain entrance control over scrambled information utilizing access approaches and attributed qualities among private keys and ciphertexts. Especially, Ciphertext-policy attribute-based encryption gives an adaptable method for scrambling information such that the encryptor characterizes the characteristic set that the decryptor needs to have with a specific end goal to unscramble the ciphertext [13].

Consequently, diverse clients are permitted to decode distinctive bits of information for every the security arrangement. On the other hand, the issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related qualities eventually (for instance, moving their area), or some private keys may be traded off, key repudiation (or redesign) for each one characteristic is fundamental to make frameworks secure. On the other hand, this issue is significantly more troublesome, particularly in ABE frameworks, since each one trait is possibly imparted by numerous clients (from now on, we allude to such a gathering of clients as a quality gathering).

This infers that renouncement of any quality or any single client in a characteristic gathering would influence alternate clients in the gathering. Case in point, if a client joins or leaves a quality gathering, the related characteristic key ought to be changed and redistributed to the various parts in the same gathering for regressive or forward mystery. It may bring about bottleneck amid rekeying system or security corruption because of the windows of powerlessness if the past property key is not overhauled promptly. An alternate test is the key escrow issue.

In CP-ABE, the key Power creates private keys of clients by applying the power’s expert mystery keys to clients’ related set of properties. In this manner, the key power can decode each ciphertexttended to particular clients by producing their trait keys. On the off chance that the key power is traded off by enemies when sent in the antagonistic situations, this could be a potential danger to the information classifiedness or security particularly when the information is exceedingly delicate.

The key escrow is an inborn issue even in the numerous power frameworks the length of each one key power has the entire benefit to produce their own particular trait keys with their own particular expert mysteries. Since such a key era instrument focusedaround the single expert mystery is the fundamental technique for the greater part of the lop sided encr-yption frameworks, for example, theproperty based or character based encryption conventions, up roo-ting escrow in single or numerous power CP-ABE is a urgent open issue.

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. 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.

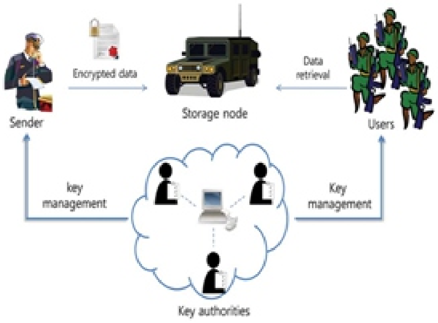
This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for 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.

PROPOSED SYSTEM:

In this paper, 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.

System Architecture:



MODULES:

1.Key Authorities
2.Storage Nodes
3.Sender
4.User

MODULES DESCRIPTION:

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.

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.

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.

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 ciphertext and obtain the data.

CP-ABE Method :

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor.

This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and builtpolicies into user's keys; while in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

RELATED WORKS:

ABE comes in two flavors called key-policy ABE (KP-ABE) and Ciphertextpolicy attribute-based encryption. In KP-ABE, the encryptor just gets to name a ciphertext with a set of attributes. thekey power picks an approach for each one client that figures out which ciphertexts he can unscramble and issues the way to every client by inserting the strategy into the client's key.

However, the parts of the ciphertexts and keys are turned around in CP-ABE.in CP-ABE, the ciphertext is encoded with a right to gain entrance arrangement picked by an encryptor, however a key is just made concerning a qualities set. CP-ABE is more proper to DTNs than KP-ABE in light of the fact that it empowers encryptors, for example, an officer to pick a right to gain entrance arrangement on credits and to encode secret information under the right to gain entrance structure by means of encoding with the comparing open keys or properties [4], [7], [15].

EXISTING FRAMEWORK:

The idea of Attribute based encryption (ABE) is a guaranteeing approach that satisfies the prerequisites for secure information recovery in DTNs. ABE characteristics a system that empowers a right to gain entrance control over scrambled information utilizing access approaches and credited qualities among private keys and ciphertexts. The issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related qualities sooner or later (for instance, moving their district), or some private keys may be traded off, key repudiation (or redesign) for each one characteristic is fundamental keeping in mind the end goal to make frameworks secure.

This infers that renouncement of any property or any single client in a characteristic gathering would influence alternate clients in the gathering. Case in point, if a client joins or leaves a trait assemble, the related characteristic key ought to be changed and redistributed to the various parts in the same gathering for retrograde or forward mystery. It may bring about bottleneck amid rekeying method or security corruption because of the windows of powerlessness if the past characteristic key is not overhauled quickly.

Disadvantages:

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.

PROBLEM DEFINITION:

The problem of applying the ABE to DTNs introduces several security and privacy challenges. 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.

CHALLENGES:

One of the main challenges 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. 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.

Key-Policy Attribute-Based Encryption (KP-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.

Attribute Revocation:

Solutions proposed to append to each attribute an expiration date or time and distribute a new set of keys to valid users after the expiration.

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 ciphertext addressed to users in the system by generating their secret keys at any time.A distributed KP-ABE scheme proposed solves the key escrow problem in a multiauthority 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.

Decentralized ABE:

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.

ABE comes in two flavors called key-policy

- ABE (KP-ABE) and
- Ciphertext-policy ABE (CP-ABE).

KP-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.

Ciphertext-policy ABE (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 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.

Attribute Revocation:

Solutions proposed 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. The first problem is the security degradation in terms of the backward and forward secrecy. The other is the scalability problem. The key authority periodically announces a key update material by unicast at each timeslot so that all of the nonrevoked 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 nonrevoked users.

The immediate key revocation can be done by revoking users using ABE that supports negative clauses. 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 of Bethencourt et al., where is the maximum size of revoked attributes set .Golle et al. also 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.

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 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 multiauthority 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 components besides the attributes keys, where is the number of authorities in the system.

Decentralized ABE:

Huang et al. and Roy et al. proposed decentralized CP-ABE schemes in the multiauthority 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 multiencrypting 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 multiencryption 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 Lewko et al. proposed multiauthority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

FUNCTIONING OF THE FRAMEWORK:

Key Powers: They are key era focuses that create open/mystery parameters for CP-ABE. The key powers comprise of a focal power and numerous neighborhood powers. We accept that there are secure and dependable correspondence channels between a focal power and every neighborhood power amid the starting key setup and era stage. Every neighborhood power oversees diverse characteristics and issues relating credit keys to clients. They give differential access rights to individual clients focused around the clients' traits. The key powers are thought frankly however inquisitive. That is, they will sincerely execute the allotted undertakings in the framework; nonetheless they might want to learn data of scrambled substance however much as could reasonably be expected.

Capacity hub:

This is a substance that stores information from senders and give comparing access to clients. It might be portable or static. Like the past plans, we additionally expect the capacity hub to be semiassumed that is fair yet inquisitive.

Sender:

This is an element who claims private messages or information (e.g., a commandant) and wishes to store them into the outer information stockpiling hub for simplicity of imparting or for dependable conveyance to clients in the amazing systems administration situations. A sender is in charge of characterizing (characteristic based) access arrangement and authorizing it all alone information by scrambling the information under the strategy before putting away it to the stockpiling hub.

Client:

This is a versatile hub that needs to get to the information put away at the stockpiling hub (e.g., a fighter). In the event that a client has a set of properties fulfilling the right to gain entrance approach of the encoded information characterized by the sender, and is not disavowed in any of the qualities, then he will have the capacity to decode the ciphertext and get the information.

CONCLUSIONS:

In this Paper we have a tendency to address a secure information retrieval theme victimization CP-ABE for suburbanized DTNs wherever multiple key authorities manage their attributes severally. We have atendency to incontestable a way to apply the projected mechanism to firmly and with efficiency manage the confidential information distributed within the disruption-tolerant military network. Disruptiontolerant network (DTN) technologies are getting booming solutions that enable wireless devices carried by troopers to speak with one another and access the wind or command faithfully by exploiting memory device nodes. a number of the foremost difficult problems during this situation square measure the social control of authorization policies and therefore the policies update for secure information retrieval. Ciphertext-policy attribute-based encoding (CP-ABE) could be apromising cryptanalytic resolution to the access management problems. However, the matter of applying CP-ABE in suburbanized DTNs introduces many security and privacy challenges with relevance them attribute revocation, key escrow, and coordination of attributes issued from completely different authorities.

REFERENCES:

[1]. JunbeomHur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks"-IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.

[2]. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309– 329,2003.

[3] S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.

[4] P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet, 2008,pp. 26–35.

[5] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE,"in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456– 465.

[6] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

[7] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertextpolicy attribute based encryption," in Proc. ASI ACCS, 2009, pp. 343–352.

[8] S. S. M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

[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.