Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

PATTAN FIROZE¹, VEERA MALLESWARARAO GALLI²

¹Assistant Professor, Dept of CSE, Velaga Nageswara Rao College of Engineering, Ponnur, Guntur, AP, India, E-mail: firoze.pattan@gmail.com.
²PG Scholar, Dept of CSE, Velaga Nageswara Rao College of Engineering, Ponnur, Guntur, AP, India, E-mail: wings.malli@gmail.com.

Abstract: In the large number of outgrowing commercial environment each and everything depends on the other sources to transmit the data securely and maintain the data as well in the regular medium. Portable nodes in military environments, for example, a front line or an antagonistic area are prone to experience undergo of irregular system network and frequent partitions. Disruption-tolerant network (DTN) innovations are getting to be fruitful results that permit remote device conveyed by officers to speak with one another and access the confidential data or secret data or summon dependably by abusing outside capacity nodes or storage nodes. Thus a new methodology is introduced to provide successful communication between each other as well as access the confidential information provided by some major authorities like commander or other superiors. The methodology is called Disruption-Tolerant Network (DTN). This system provides efficient scenario for authorization policies and the policies update for secure data retrieval in most challenging cases. The most promising cryptographic solution is introduced to control the access issues called Cipher text Policy Attribute Based Encryption (CP-ABE). Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. 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. 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 safely and proficiently deal with the classified information dispersed in the Interruption or disruption tolerant network.

Keywords: Access Control, Attribute-Based Encryption (ABE), Disruption-Tolerant Network (DTN), Multi-Authority, Secure Data Retrieval.

I. INTRODUCTION

The design of the current Internet service models is based on a few assumptions such as (a) the existence of an end-to-end path between a source and destination pair, and (b) low round-trip latency between any node pair. However, these assumptions do not hold in some emerging networks. Some examples are: (i) battlefield ad-hoc networks in which wireless devices carried by soldiers operate in hostile environments where jamming, environmental factors and mobility may cause temporary disconnections, and (ii) vehicular ad-hoc networks where buses are equipped with wireless modems and have intermittent RF connectivity with one another.

Fig.1. Military Networks.

In the above scenarios, an end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic, predictably connectable, or periodically connected. To allow nodes to communicate with each other in these extreme networking environments, Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other as shown in Fig.1. 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. After the connection is eventually established, the message is delivered to the destination node. 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 (e.g., the attribute representing current location of moving soldiers) [5], [9], [10]. We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN [11].

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. In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user’s private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt.

Our scheme can provide not only fine-grained access control to each content object but also more sophisticated access control antics. Ciphertext-policy attribute-based encryption (CP-ABE) is a guaranteeing cryptographic answer for the right to gain entrance control issues. In any case, the issue of applying CP-ABE in decentralized DTNs presents a few securities and protection challenges as to the property disavowal, key escrow, and coordination of characteristics issued from distinctive powers. 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 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 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 attributes 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. 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, encryptions 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.
Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

II. EXISTING AND PROPOSED SYSTEMS

A. 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, cipher text-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 decrypt the cipher text. Thus, different users are allowed to decrypt different pieces of data per the security policy.

Disadvantages of Existing System:
- 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, we refer to such a collection of users as an attribute group)
- 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.
- The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes 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.

B. 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 as shown in Fig.2.

Advantages of Proposed System:
- 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.
- 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.
- 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.

C. System Architecture

Fig.2. Architecture of secure data retrieval in a disruption-tolerant military network.

D. Modules
- Key Authorities
- Storage Nodes
- Sender
- User

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.
PATTAN FIROZE, VEERA MALLESWARARAO GALL

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 cipher text and obtain the data.

III. 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 cipher text with a set of attributes. The key 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 cipher text 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.

Trait Disavowal: initially recommended key disavowal instruments in CP-ABE and KP-ABE, individually. Their answers are to affix to each one characteristic a termination date (or time) and disperse another set of keys to substantial clients after the close. The occasional property revocable ABE plans have two primary issues. The principal issue is the security corruption regarding the retrograde and forward mystery. It is a respectable situation that clients, for example, fighters may change their qualities frequently, e.g., position or area move when considering these as characteristics. At that point, a client who recently holds the credit may have the capacity to get to the past information encoded before he gets the quality until the information is re-encrypted with the recently upgraded characteristic keys by occasional rekeying (regressive secrecy).for sample, expect that at a time, a cipher text is scrambled with an approach that might be unscrambled with a set of qualities (implanted in the clients keys) for clients with. After time, say, a client recently holds the quality set. Regardless of the possibility that the new client ought to be refused to decode the cipher text for the time example, he can at present unscramble the past cipher text until it is re-encrypted with the recently upgraded quality keys. Then again, a renounced client would in any case have the capacity to get to the scrambled information regardless of the possibility that he doesn't hold the quality any more until the following lapse time.

IV. 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 [10] and RC [5] 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. Therefore, attributes of users can be revoked at any time even before the expiration time that might be set to the attribute. This enhances security of the stored data by reducing the windows of vulnerability. In addition, the proposed scheme realizes more fine-grained user revocation for each attribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the cipher text. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Authority</th>
<th>Expressiveness</th>
<th>Key Escrow</th>
<th>Revocation</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSW [13]</td>
<td>single</td>
<td></td>
<td>yes</td>
<td>periodic attribute revocation</td>
</tr>
<tr>
<td>HV [9]</td>
<td>multiple</td>
<td>AND</td>
<td>yes</td>
<td>periodic attribute revocation</td>
</tr>
<tr>
<td>RC [4]</td>
<td>multiple</td>
<td>AND</td>
<td>yes</td>
<td>immediate system-level user revocation</td>
</tr>
<tr>
<td>Proposed</td>
<td>multiple</td>
<td>any monotone access structure</td>
<td>no</td>
<td>immediate attribute-level user revocation</td>
</tr>
</tbody>
</table>

International Journal of Innovative Technologies
Volume.04, Issue No.07, June-2016, Pages: 1203-1209
Table II summarizes the efficiency comparison results among CP-ABE schemes. In the comparison, rekeying message size represents the communication cost that the key authority or the storage node needs to send to update non-revoked users’ keys for an attribute. Private key size represents the storage cost required for each user to store attribute keys or KEKs. Public key size represents the size of the system public parameters. In this comparison, the access tree is constructed with attributes of m different authorities except in BSW of which total size is equal to that of the single access tree in BSW. As shown in Table II, the proposed scheme needs rekeying message (Hdr) size of at most \( (n-l) \log_2 n \) to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its cipher text size is linear to the number of revoked users in the system since the user revocation message is included in the cipher text. The proposed scheme requires a user to store \( \log n \) more KEKs than BSW. However, it has an effect on reducing the rekeying message size. The proposed scheme is as efficient as the basic BSW in terms of the cipher text size while realizing more secure immediate rekeying in multi-authority systems.

**B. Simulation**

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption.

The number of users joining a group follows a Poisson distribution with rate \( \lambda \), and the membership duration time follows an exponential distribution with a mean duration \( 1/\mu \). Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution. We suppose that user join and leave events are independently and identically distributed in each attribute group following Poisson distribution the membership duration time for an attribute is assumed to follow an exponential distribution. Almeroth and Anmar demonstrated the group behavior in the Internet’s multicast backbone network (MBone). We set the inter arrival time between users as 20 min (\( \lambda = 3 \)) and the average membership duration time as 20 h (1/\( \mu = 20 \)). Fig. 3 represents the number of current users and revoked users in an attribute group during 100h. Fig4 shows the total communication cost that the sender or the storage node needs to send on a membership change in each multi-authority CP-ABE scheme. It includes the cipher text and rekeying messages for non-revoked users. It is measured in bits. In this simulation, the total number of users in the network is

### TABLE III: Comparison Of Computation Cost

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Pairing</th>
<th>Exp. in G0</th>
<th>Exp. in G1</th>
<th>Computation (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSW [13]</td>
<td>S</td>
<td>2k + 1</td>
<td>1</td>
<td>2 + 1.2</td>
</tr>
<tr>
<td>HIV [9]</td>
<td>U</td>
<td>2t + 1</td>
<td>( \log t )</td>
<td>5.8k + 0.2logt + 2.9</td>
</tr>
<tr>
<td>RC [4]</td>
<td>S</td>
<td>2k + m</td>
<td>mlog(t/m)</td>
<td>8.8k + 2.9m + 0.2log(t/m) + 2.9</td>
</tr>
<tr>
<td>Proposed</td>
<td>S</td>
<td>2k + 1</td>
<td>( k \log t )</td>
<td>6.8k + 0.2logt + 2.9</td>
</tr>
</tbody>
</table>

S: sender, U: user

---

*Fig. 3. Number of users in an attribute group.*

*Fig. 4. Communication cost in the multi-authority CP-ABE systems.*
10,000, and the number of attributes in the system is 30. The number of the key authorities is 10, and the average number of attributes associated with a user’s key is 10. For a fair comparison with regard to the security perspective, we set the rekeying periods in HV as 1/\lambda \text{ min}. To achieve an 80-bit security level, we set C_0 = 512, C_p = 160. \text{ct} is not added to the simulation result because it is common in all multi-authority CP-ABE schemes. As shown in Fig. 4, the communication cost in HV is less than RC in the beginning of the simulation time (until around 30h). However, as the time elapses, it increases conspicuously because the number of revoked users increases accumulatively. The proposed scheme requires the least communication cost in the network system since the rekeying message in Hdr is comparatively less than the other multi-authority schemes.

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) providing groups in which a bilinear map \( e: G_0 \times G_0 \rightarrow G_1 \) is 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 \( G_0 \) needs 512 bits at an 80-bit security level and 1536 bits when 128-bit of security are chosen. Table III shows the computational time results. For each operation, we include benchmark timing. Each cryptographic operation was implemented using the PBC library ver. 0.4.18 on a 3.0-GHz processor PC. The public key parameters were selected to provide 80-bit security level. The implementation uses a 160-bit elliptic curve group based on the super singular curve \( y^2 = x^3 + x \) over a 512-bit finite field. The computational cost is analyzed in terms of the pairing, exponentiation operations in \( G_0 \) and \( G_1 \). The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the cipher text is a complete binary tree. Computation costs in Table III represent the upper bound of each cost. We can see that the total computation time to encrypt data by a sender in the proposed scheme is the same as BSW, while decryption time by a user requires \( k \) exponentiations in \( G_0 \) more. These exponentiation operations are to realize the fine-grained key revocation for each attribute group. Therefore, we can observe that there is a tradeoff between computational overhead and granularity of access control, which is closely related to the windows of vulnerability. However, the computation cost for encryption by a sender and decryption by a user are more efficient compared to the other multi-authority schemes.

V. CONCLUSION

Our project is not the unique one, but is an endeavor attempt to have a precise scenario of what the terms “secure data retrieval for decentralized disruption tolerant network” is meant to be and its. 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.

Implementation as well on which we are currently working as stated before, our proposed system can enhance the security of military network by using CP-ABE mechanism. CP-ABE is a scalable cryptographic solution to the access control and secures 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.

VI. REFERENCES
