Implementation of Decentralized Disruption-Tolerant Network Based on Secure Data Retrieval Technique for Military Network Applications

DR. SHOEBS PEEY SYED1, PROF. SHAHIM PASH2
1E-mail: shoebapcs@gmail.com & 2E-mail: safa.pasha@gmail.com.

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. Cipher text-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.

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

I. 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 [2]–[4]. 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. Roy [5] and Chuah [6] 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 [7], [8]. 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 concept of attribute-based encryption (ABE) [12] 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. 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, we 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.

Copyright © 2015 IJATIR. All rights reserved.
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 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.

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 encrypt 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, 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 as shown in Fig.1. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with
Implementation of Decentralized Disruption-Tolerant Network Based on Secure Data Retrieval Technique for Military Network Applications

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 of Proposed System:
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.

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.

C. System Architecture

Fig.1. Architecture of secure data retrieval in a disruption-tolerant military network.

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

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 example, 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 I: Expressiveness, Key Escrow, and Revocation Analysis**

<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 [3]</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>any monotone access structure</td>
<td>n</td>
<td>immediate attribute-user level revocation</td>
<td></td>
</tr>
</tbody>
</table>

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-1) log \( \frac{n}{m-1} C_p \) 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 revocation in multi-authority systems.

**B. Simulation**

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar demonstrated the group behavior in the Internet’s multicast backbone network (MBone). They
Implementation of Decentralized Disruption-Tolerant Network Based on Secure Data Retrieval Technique for Military Network Applications

showed that 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

$$\text{Fig. 2. Number of users in an attribute group.}$$

and rekeying messages for non-revoked users. It is measured in bits. In this simulation, the total number of users in the network is 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 $C_0 = 512$, $C_p = 160$. $C_T$ is not added to the simulation result because it is common in all multi-authority CP-ABE schemes. As shown in Fig. 3, the communication cost in HV is less than RC in the beginning of the simulation time (until about 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.

**TABLE III: Comparison of Computation Cost**

<table>
<thead>
<tr>
<th>Time (ms)</th>
<th>Pairing</th>
<th>Exp. in $C_0$</th>
<th>Exp. in $C_p$</th>
<th>Computation (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.9</td>
<td>1.0</td>
<td>0.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSW</td>
<td>S</td>
<td>$2t + 1$</td>
<td>$\log t$</td>
<td>$2t + 1.2 + 2.9$</td>
</tr>
<tr>
<td>[13]</td>
<td>U</td>
<td>$2t + 1$</td>
<td>$\log t$</td>
<td>$2t + 1.2 + 2.9$</td>
</tr>
<tr>
<td>HV</td>
<td>S</td>
<td>$2k + m$</td>
<td>$\frac{\log(t/m)}{m}$</td>
<td>$2t + 1.2 + 2.9$</td>
</tr>
<tr>
<td>[9]</td>
<td>U</td>
<td>$2k + m$</td>
<td>$\frac{\log(t/m)}{m}$</td>
<td>$2t + 1.2 + 2.9$</td>
</tr>
<tr>
<td>RC</td>
<td>S</td>
<td>$2t + 1$</td>
<td>$\log t$</td>
<td>$3t + 1.2$</td>
</tr>
<tr>
<td>[4]</td>
<td>U</td>
<td>$2k + m$</td>
<td>$\frac{\log(t/m)}{m}$</td>
<td>$8.7t + 2.9m + 0.2\log(t/m)$</td>
</tr>
<tr>
<td>Proposed</td>
<td>S</td>
<td>$2t + 1$</td>
<td>$k$</td>
<td>$2t + 1.2$</td>
</tr>
<tr>
<td></td>
<td>U</td>
<td>$2k + 1$</td>
<td>$\log t$</td>
<td>$6.8t + 0.2k + 2.9$</td>
</tr>
</tbody>
</table>

S: sender, U: user

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

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 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