Secure Data Retrieval for Spread out Commotion Forbearing Military Networks

Ranjani S.[1], Kavitha N. S.[2]
[2]*Faculty,*[1,2]*Department of Computer Science and Engineering*
[1,2]*Erode Sengunthar Engineering College, Erode, Tamilnadu, India*

Abstract - Mobile nodes in challenging network scenarios such as military networks are likely suffer from intermittent network connectivity ie., the signals are stopping and starting at regular intervals. Disruption-tolerant network (DTN) technology is used to overcome this problem. It allows accessing the wireless devices and confidential information reliably. The confidential information must be securely retrieved. The key issues are enforcement of authorization policies update for secure data retrieval. The Ciphertext Policy Attribute-Based Encryption (CP-ABE) is the best solution to the access control issues. Privacy and security challenges which include key escrow, attribute revocation can be resolved by using CP-ABE. We propose a secure data retrieval scheme which is based on CP-ABE approach. Our scheme provides flexible fine-grained access control such that the encrypted data can only be accessed by the authorized users. Multiple key authorities manage their attributes independently and the party determines the access policy while data encryption. The encrypted data involves decryption by the user only if the user satisfied the access policy. We express how securely the confidential data is retrieved in disruption tolerant network.

Keywords: Access control, disruption-tolerant networking, secure data retrieval, CP-ABE.

I. INTRODUCTION

In many network scenarios such as battlefield, connections of wireless devices carried by armed forces may be momentarily disconnected by congestion, environmental factors, and mobility, especially when they work in unfriendly environments. Disruption- tolerant network (DTN) technology[1] provides a successful solution that allows nodes to be in touch with each other in these extreme unreceptive networking environments. Normally, when the source and a target pair does not have an end-to-end connection pair, the messages from the source node may need to wait in the intermediate nodes for a considerable amount

of time until the connection would be finally established. Attribute-based encryption (ABE) concept fulfills the requirements for data retrieval in DTN mostly, ciphertext-policy ABE (CP-ABE) provide a scalable way of encrypting the data[7]. Thus, different users are allowed to decrypt different pieces of data per the security policy which is determined by the sender.

A. Disruption Tolerant Network (DTNS)

Disruption Tolerant Networks (DTNs) allow for routing in networks where the source to destination paths is unstable. Unstable paths results in several challenges at the link layer. For example: denial-of-attack, the range of radio waves are too short, node mobility may be high, and node density is low, environmental interference. In undeveloped areas such environments can exist and those problems occur when stable connections are destroyed due to natural disaster.

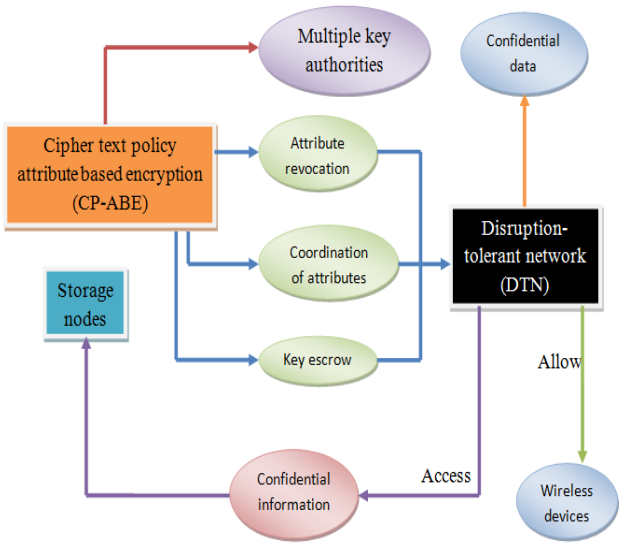

Fig 1.1 Data flow in DTN allowing wireless device

Disruption tolerant network can be based on moving nodes such as vehicles or pedestrians. Disruption tolerant network technology is widely used to prevail over the problem occurred in the following environment:

(1) Asymmetric data rate

(2) Long delay

(3) Intermittent connectivity

(4) High Error rate

In many application DTN technology is used. Mainly in military and intelligence DTN is used for wireless communication, monitoring. DTN supports interoperability of other networks by accepting long disruptions and delays within the networks.

B. Ciphertext Policy Attribute-Based Encryption (CP-ABE)

Ciphertext policy Attribute-based Encryption (CP-ABE) is a public-key cryptography that was planned to determine the exact problem of fine-grained access control on mutual data in one-to-many connections. CP-ABE provides a way of encrypting the data such that an encryptor specifies the access policy. The user must satisfy the access policy in order to decrypt the data. In CP-ABE scheme, each user have a private key, associated with set of attributes which describing the user and a encrypted cipher text. It specifies an access policy over attributes. At present, the only method for enforcing those policies is to utilize a trusted server to store the data. On the other hand, if the trusted server storing the confidential data is compromised, then the data is not confidentiality. This work presents a system for complex access control on the data which is encrypted that call Ciphertext Policy Attribute-Based Encryption (CP-ABE). By using this technique the data which is in encrypted form can be kept confidential even if the data stored in the server is compromised, this method is mainly secure against collusion attacks.

II. System Model

In this paper, we propose secure data retrieval using ciphertext policy attribute-based encryption in distributed military networks based on the user attributes. The forward and backward secrecy of the data can be reduced by attribute revocation. Encryptors determine a fine-grained access policy for the decryptor[8]. By performing 2PC (two-party communication) protocol the key issuing protocol generates the key and issue it among the key authoritites. The access policy defined by the must be satisfied by the user to decrypt the confidential data. The main trouble is in conditions of security. The soldiers may modify their attributes usually for ex., soldiers may move from one place to another and the attributes might be changed. The attributes of the soldier must be regularly updated. This is not easy in ABE because each attribute is shared by multiple users.

A. System Architecture

In this part, we illustrate the entire system architecture and its security model.

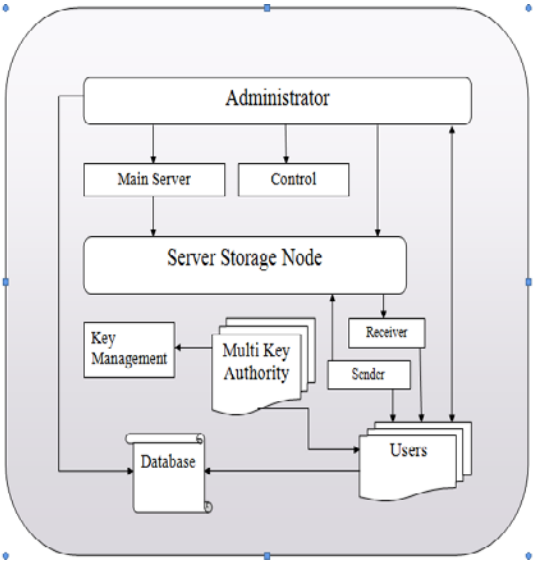

Fig 2.1 Architecture of secure data retrieval for spread out commotion forbearing military networks

B. System Description

Fig 2.1 shows the architecture of secure data retrieval for spread out commotion forbearing military networks. The system architecture consists of the following entities.

1. Key Authorities: Key authorities consists of central authority and multiple local authority[6]. Key authorities are responsible for generating the keys. We made an assumption that the connection is secure in between the central authority and each local authority and the connections are reliable. It well improves the security and preventing from unauthorized user enters into the network.
2. Storage node: Storage node stores all the data from the sender. The users has right to use the data from the storage node. Storage node is to be not fully-trusted. Storage node can get the data without traffic and also transmit the data in less time.
3. Store-carry and forward: For ease of sharing or for reliable delivery to users, the commander wishes to store confidential messages or data into the external data storage node in the hostile environments.

4. Distributed User: Here there is decentralized network. Each user has rights to use the data from any user[9]. The secret data can be accessed quickly and consistently. Thus the scalability and protection can be improved.
5. Analysis: This entity shows the development of overall process in two-party communication protocol for sharing the confidential data. It shows the size of the confidential data and the time it delivers to the corresponding users accurately.

III. PREVIOUS WORK

J**. Bethencourt, A. Sahai, and B. Waters(2007)** proposed **Ciphertext policy attribute based encryption**

In several distributed systems a user hold only be able to access data if a user posses a certain set of credentials or attributes. However, if any server storing the data is compromised, then the secret of the data will be compromised. To overcome this problem, a technique called Ciphertext-Policy Attribute-Based Encryption was proposed[2]. The cpabe package, which has been made available on the web under the General Public License. The functioning was done using the Pairing Based Cryptography (PBC) library. This cpabe toolkit provides four command line tools:

- cpabe-setup which generates a public key and a master key.
- cpabe-keygen where a master key is given and it generates a private key for a set of attributes.
- cpabe-enc where a public key is given and it encrypts a file under an access tree specified in a policy language.
- cpabe-dec where a private key is given and it decrypts a file.

M. Chase (2007) proposed **Multi authority attribute based encryption**

Each user is identified by a unique personality string. An Attribute Based Encryption scheme (ABE), is a scheme in which each user is identified by a set of attributes, and some of those attributes is used to determine the decryption ability for each ciphertext. Single authority attribute encryption was used[3]. SW technique allows multi-authority attribute based encryption. This scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. This scheme can tolerate an arbitrary number of corrupt authorities. SW scheme is in which a sender can encrypt a message specifying an attribute set and a number d so that only a recipient who has at least dk of the given attributes can decrypt the message. This technique allow the sender to specify for each authority k a set of attributes monitored by that authority and a number dk so that the message can be decrypted only by a user who has atleast dk of the given attributes from every authority. The technique used required that every user have some kind of a global identifier (GID). It require only two properties from this:

- No user can claim another user's identifier
- All authorities can authenticate a user's identifier.

S. Yu, C. Wang, K. Ren, and W. Lou (2010) proposed **Attribute based data sharing with attribute revocation**

Ciphertext-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for fine-grained access control for data sharing. In CP-ABE, each user is associated with a set of attributes and data are encrypted with access structures based on attributes. A user is capable to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. To secure the confidential data they use the technique called Proxy Re-Encryption (PRE) technique[13]. A Proxy Re-Encryption Technique scheme allows the proxy, using the proxy re-encryption key, to convert ciphertexts under public key pka into cipher- texts under public key pkb and vise versa.

This scheme is composed of 7 algorithms: Setup, Encryption, KeyGeneration, ReKeyGeneration, ReEncryption, ReKey, and Decreption. Setup, KeyGeneration, and ReKeyGeneration are performed by the authority while ReEncryption and ReKey are executed by proxy servers. Encryption and Decryption are called by encryptors and decryptors respectively.

Whenever an attribute revocation event occurs, the authority redefines the master key components for involved attributes. For this purpose, the authority generates proxy rekey's for updated master key mechanism[13]. Using these proxy re-key's, the proxy servers are able to securely update user secret keys. The proxy re-key's also allow the proxy servers to re-encrypt existing ciphertexts stored on them. The main advantage of this scheme is that it places minimal load on authority upon attribute revocation events.

S. Roy and M. Chuah (2009) proposed **Secure data retrieval based on ciphertext policy attribute based encryption system for the DTNs**

Mobile node in some network scenarios suffer from intermittent connectivity and frequent partitions. Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. It has privacy

challenge as attribute revocation. Revocation is even more challenging in attribute-based systems. Each attribute probably belongs to multiple different users, whereas in traditional systems public/private key pairs are uniquely associated with a single user. To overcome this problem an access control method which is based on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach was proposed[11].

It provides two unique features:

- The integration of dynamic attributes[4] whose value may change over time
- The revocation feature

In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generate. Under an access policy the contents are encrypted. If a user join or leave, then the attribute of the user must be added or revoked accordingly. Thus it prevents revoked user to access the confidential data and new user can access the data easily.

In military networks the information sent between the commander and the soldiers are confidential. If the confidential data are accessing by the unauthorized users then it leads to high delay and intermittent connectivity. Each one having the separate access policy and the access control. CP-ABE is a promising cryptographic solution to the access control issues. It includes several security and privacy challenges such as attribute revocation, keyescrow and coordination of attributes.

In Ciphertext Policy Attribute-Based Encryption (CP-ABE), each user is associated with a set of attributes and data are encrypted with access policies on attributes. Existing ABE schemes depending on a single key authority suffer from the key escrow problem [11]. Each algorithm has its own advantage and disadvantages.

The problems are summarized as follows:

- Threat to the data confidentiality or privacy.
- Hard to define fine-grained access policies.
- Required increased protection of confidential data.

IV. PROPOSED METHODOLOGY

In existing system, Attribute Based Encryption is used in Disruption Tolerant Network. The problem of applying ABE to DTN introduces several security and privacy challenges. Since some users may change their attributes at some point, key revocation for each attribute is necessary in order to make system secure. Since each attribute is conceivably shared by multiple users. There is a threat to confidential data and hard to define fine-grained access policy. While transferring the confidential data from sender to receiver it has increased high delay because of easy spreading of unauthorized access. So this system requires more protection and security.

In proposed system, an exclusive mechanism was developed, that can effectively gives more protection on confidential data. A new technique called Extended Ciphertext-Policy Attribute Based Encryption is designed to give more security on confidential data, which is transferred in military environment. Key authority generates the key by using anyone of their information. Multiple key authorities manage their attributes independently. Each attribute key of a user can be updated individually and immediately. The commander and the soldier receive the data by giving the public and private key. It will give fine grained access policy. It prevent unauthorized user to access the confidential data. We provide a multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs. 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 instantaneously. Thus, the scalability and protection of the data can be enhanced in the proposed scheme. Communicate with every user in network.

The key generation consists of local authority who generates key to the user and the central authority who generates key for the local authority. The user key has one personal key and multiple attribute keys. Each user has unique personal key to avoid the collusion attack among the other users. Here two-party communication (2PC) protocol is used to avoid the key escrow problem so that any of the user cannot determine the key components of any individual user. The local and central authority is responsible for the personal key

generation. The central authority authenticate a user and select random exponent value x1.....xn where x is random number for local authority. This value is unique and personal key for the user.

The attribute key generation is done only after setting the personal key component. Using the parameter received from the central authority, the local authority generates the key for the user. The secret key for each user is calculated as:

$$SK=M=g^{((x1+....+xn)+p)/n}$$

Where x1+...+xn is the random number chosen by the central authority for every local authority. Using this, the cost for communication between tow nodes is very low. So it overhead the communication cost during the updating of the key.

Encryption: When the sender sends the confidential on the network it must by encrypted with the secret key and convert the plain test into ciphertext so that it must be protected from unauthorized users to access the data even if the storage node is compromised. The encryption is done by using the message M, private key PK of each local authority. After encrypting the data, the encrypted data is stored in the storage node.

If any of the user send the request to the storage node for encrypted data, it checks the user and if the user is validated then the encrypted data sends to the requested user.

Decryption: After getting the ciphertext from the storage node the user able to decrypt the confidential data which is in encrypted form by using the user's secret key. For decryption it has the encrypted data that is cipher text CT, secret key SK and node x. The user can able to decrypt the data if he satisfies the access structure.

Store carry and forward: 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.

If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and in any of the attributes is not revoked, then he will be capable to decrypt the ciphertext and obtain the data.

Key update and Revocation: The key should be updated to avoid the user by accessing the previous data. When a user send a join request or leave request for group the key update procedure is launched. When a user send a request to access the confidential data the storage node responds with the newly updated key.

V. Simulation/Experimental Results

At any time the users can be revoked before the revocation time. Even though the user drop any attribute or hold it he can access the confidential data with other some valid attributes which satisfying the access policy. The confidential data would be protected by resolving the key escrow problem. The communication cost can be calculated for encrypting and decrypting the data. By using the attribute group key distribution protocol the key is indefinitely secure. Since the storage node is not trusted the multiple key authorities are also no longer trusted.

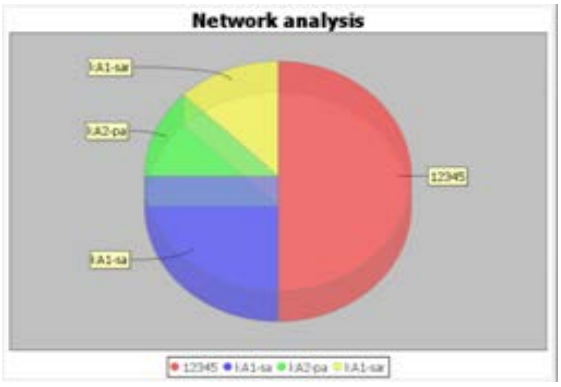

Fig 5.1 Analysis of each user in a group

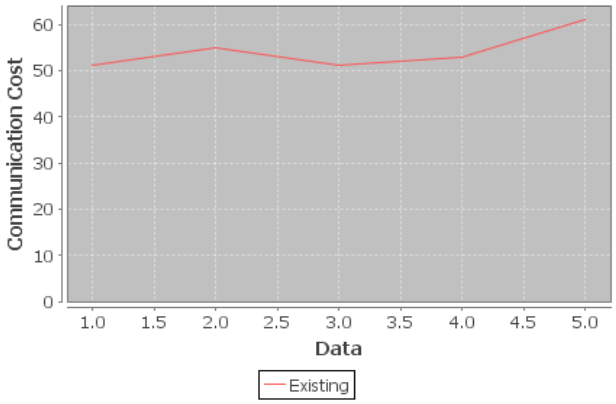

Fig 5.2 Communication cost

If the user cannot satisfy the access policy then he cannot able to access the confidential data during the decryption process. Though the storage node manages the attribute key

it cannot be able to decrypt the confidential data of any node. Because authorized users only decrypt the ciphertext by using the attribute key.

VI. CONCLUSION

In this system, the data must be transferred securely in between the commander and the soldier in the military environment and also to prevent unauthorized users to access the data. While transferring the confidential data from commander to soldier it has increased high delay because of easy spreading of unauthorized access. So this system requires more protection and security. CP-ABE is a cryptographic solution for the access control and secure data retrieval. Key authority generates the key by using anyone of their information. Multiple key authorities manage their attributes independently. Each attribute key of a user can be updated individually and immediately. It provides fine-grained access control to the user. The confidentiality of the stored data is guaranteed even under the challenging environment.

VII. FUTURE SCOPES

CP-ABE algorithm provides fine-grained access control to the user and prevents unauthorized user to access the confidential data. The storage node is used to maintain all the information about the users and the sender. It can be extended in the future work about to improve the attribute of revocation for identifying the user if he wants to remove from the group, can extends user validation for set of attribute in authentication of multiauthority network environment. The trusted authority is analysis by values of distributed identically. The details of the user must be updated in the database at regular intervals such that the information about the user alive details etc.

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] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

[3] M. Chase and S. S. M. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

[4] 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

[5] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in Proc. IEEE MILCOM, 2007, pp. 1–7

[6] M. Chase, “Multi-authority attribute based encryption,” in Proc. TCC, 2007, LNCS 4329, pp. 515–534.

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

[8] 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.

[9] Junbeom Hur and Kyungtae kang, “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”, in Proc IEEE Trans on Networking 2014, Vol 22, No. 1.

[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secure attribute based systems,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.

[11] 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

[12] A. T. Sherman and D. A. McGrew, “Key establishment in large dynamic groups using one-way function trees,” IEEE Trans. Softw. Eng., 2003,vol. 29, no. 5, pp. 444–458.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. ASIACCS, 2010, pp. 261–270.