A Novel Technique for Secure Data Retrieval

Sarika Sugunan
Computer Science and Engineering, KMEA Engineering College, Ernakulam, India

Arifa Azeez
Computer Science and Engineering, KMEA Engineering College, Ernakulam, India

Abstract: Mobile nodes in a hostile network are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming a productive solution that allow wireless devices to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. The most critical issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval in wireless networks. Ciphertextpolicy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access management problems. 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 work, we propose a secure data retrieval scheme using CP-AUBE for decentralized DTNs where multiple key authorities manage their multiple attributes independently. Also we enforce a group oriented attribute based encryption and also incorporate an efficient attribute and key renewal technology. The group oriented encryption is done with concept of Bucketization which produces an optimal solution. Hence the proposed mechanism demonstrates how to securely and efficiently manage the confidential data distributed in the disruption-tolerant network.

Keywords: Attribute, Disruption-tolerant network, Attribute, Bucketization.

1. INTRODUCTION

In many network scenarios connections of wireless devices may be temporarily disconnected by factors such as jamming, environmental factors and mobility, particularly when they operate in hostile situations. Disruption tolerant network (DTN) technologies have become successful solutions that allow nodes to communicate with each other in these extreme networking environments. A disruption-tolerant network (DTN) is a network architecture that reduces intermittent communication issues by addressing technical problems in heterogeneous networks that lack continuous connectivity.

Specifically when there is no end-to-end connection between a source and a destination pair then 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. In such a scenario, introduced storage nodes in DTNs where data is stored or replicated such that only authorized nodes can access the necessary information quickly and efficiently. Several military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In such 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.

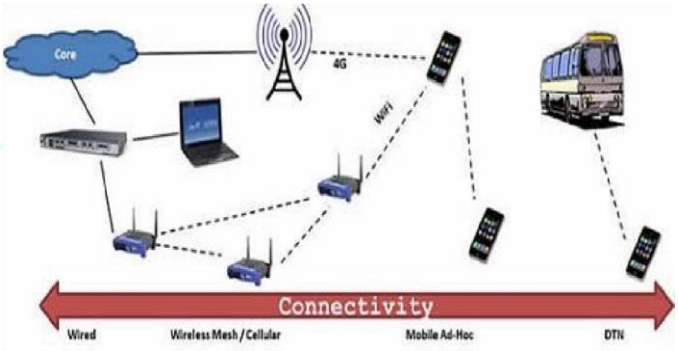

Fig 1 Disruption-Tolerant Networks

For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node that may 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 modified (e.g., an attribute representing the current location of moving soldiers in a battlefield). We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

The concept of attribute-based encryption (ABE) is a promising approach that satisfies the necessities for secure data retrieval in DTNs. ABE options a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among ciphertexts and private keys. Especially, ciphertext-policy ABE (CP-ABE) provides a flexible way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Hence different users are allowed to decrypt different pieces of data per the security policy.

ABE can be categorized in to two types depending on whether the attributes are embedded in the ciphertext or whether the access-structure is embedded in the ciphertext. The first is the Key-policy based ABE (KP-ABE) which was in fact the initial form of attribute based encryption that was developed. In KPABE they encrypt the attributes along with the data and give the access structure to each user as part of their secret key. But attribute based encryption is more applicable in the regular world if the access structure can be embedded in the ciphertext and the users can have their attributes saved in their secret keys and such a form of ABE is known as ciphertextpolicy based (CP-ABE) and was introduced by Bethencourt et al. Both these initial schemes were largely based on the secret sharing scheme. However, it is ciphertext policy based ABE that has become more popular in later schemes. This might be largely due to the fact that CP-ABE represents a natural and more intuitive way to view attributes based encryption.

While current private key cryptosystems such as AES are believed to be mathematically secure but they are only as secure as their keys are. Any user with the encryption key is able to decrypt and subsequently access the data. This proves difficult when needing to authorize a large group of individuals to decrypt the data, as any of the users has a chance to act maliciously and distribute the key, enabling unauthorized individuals to decrypt and access the data. To improve the security of such scenarios is to provide a scheme which presents each user with a personal key used for decryption. Ciphertext-Policy Attribute Based Encryption (CPABE) fits this desire exactly. It allows each user to have a unique key, which is defined by their properties CPABE was not the first cryptosystem satisfying these criteria, with its roots based in Identity Based Encryption (IBE), which was originally proposed by Shamir in 1984.

Shamir‟s original IBE scheme was designed to allow encryption and signature verification between two users without any exchange of keys, instead using a trusted server to generate unique keys for each user. Instead of directly having users handle keys, personal information unique to a user, such as address, social security number, name, or a combination of such, were used as the public key. When joining the network, the user would be issued a personal smartcard that contains their private key. The main advantage to this system over other public key infrastructure (PKI) implementations is that subsequent communications did not require any access to such infrastructure.

Sahai and Waters improved on this scheme, which transformed a user‟s identity from a single string into a set of attributes, as well as adding an error tolerance, which allowed a user to decrypt an encrypted file if their attributes were within a small difference. An additional desire of this system was to ensure that users could not collude and combine single attributes to decrypt a plaintext requiring both and they also wished to minimize the overall size of the private keys. This is the first known example of Attribute-Based Encryption (ABE), and presented much of the underlying architecture for CPABE, as the decryption steps are similar, however restricted to a single level of access trees.

Goyal et al. provided a more expressive modification to ABE, called Key-Policy Attribute-Based Encryption (KPABE) which modifies the original ABE scheme to allow the user‟s private key to contain the access structure of multiple levels of properties, while the encrypted texts contain a set of attributes or flags that are used to check if the key‟s access tree is satisfied.

The main issue with KPABE is the fact that the control of the access to the encrypted data is only controlled by the attributes given to the file, and not a controlled access tree. A user encrypting a text in a KPABE scheme has no control over sets of attributes, and this makes fine control of access requiring multiple properties challenging. This is one of the reasons that led to the design of CPABE, as CPABE allows the desired attributes to be set by the user encrypting data with finegrained control, while the key generation consists of issuing properties which cannot be directly connected to a specific ciphertext. An additional restriction of KPABE is the fact that all attributes must be made public, as they are each a component of the public key. So the major issue with CPABE is the lack of key management, which goes against the goals of CPABE.

As mentioned previously, one of the major issues with CPABE is the lack of key management, which goes against the goals of CPABE. This produces a challenge when attempting to revoke and prevent a user from using a key. Additionally, paired with revocation of keys is the fact that in order to replace a key that is no longer valid, users need to go through some sort of renewal process, for either the full key, or only corresponding to specific attributes.

The proposed system removes key escrow problem during the key generation and also do an immediate user revocation on every attribute set at the same time as taking complete advantage of the scalable access control. Also we ensure an efficient attribute renewal, key updation and it also supports group oriented attribute based encryption using the concept of bucketization. As a result, the proposed system achieved more secure and elegant data access control in the disruption tolerant networks.

2. RELATED WORKS

In paper [1] they 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, encryptor 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.

This paper proposes [2] a way to construct a CP-ABE scheme which supports the use of positive and negative attributes. This modifies the CP-ABE construction to accommodate a non-monotonic access structure. In a CP-ABE cryptosystem, a plaintext M is encrypted based on an access tree structure T to generate a ciphertext CT. So the private key of user X is identified with the set of X"s attributes, S_X. A private key, SK will be able to decrypt CT if the set of attributes, S_X assigned to SK satisfies the access tree T. The scheme uses both positive attributes (e.g. „Commander") and negative attributes (e.g. „NOT Mission 2") and it should be present in T. However, private key components are only assigned to positive attributes. That means for any X, S_X does not contain any negative attribute.

In [4], the authors considers the storage node placement problem in sensor networks with the aim of minimizing the total energy cost for gathering data to the storage nodes and replying queries. They consider both fixed and dynamic tree models. They give an exact solution for fixed tree model, on how to place storage nodes to minimize total energy cost. In the dynamic tree model, they allow each sensor node to select the storage node for storage with respect to the minimal communication cost for data forwarding and query diffusion, and reply once the storage nodes have been positioned.

The paper [3], designs a content-based information retrieval system for disruption tolerant networks. The design consists of three main components such as data caching, query dissemination and message routing. Security design for such a system is also very important but in this paper they focus on data caching, and they explore two data caching schemes, namely K-copy random caching and K-copy intelligent caching.

3. PROPOSED SYSTEM

The proposed system consists of algorithms such as the Setup, Key generation, Encrypt and Decrypt

1. Setup: This is a randomized algorithm that takes input as a security parameter and outputs the public parameters PK. Encryption is done by PK and is used to generate user secret keys and is known only to the central authority.

2. Encryption: This is a randomized algorithm that takes message M as input , an access policy, and the public parameters PK. Then it outputs the ciphertext CT.

3. KeyGen: This is a randomized algorithm that takes set of a user (say X)"s attributes SX as input, a random value and outputs a secret key SK that identifies with SX.

4. Decryption: This algorithm takes the ciphertext CT as input, a secret key SK for an attribute set SX. If SX satisfies the access structure embedded in CT, it will return the original message M.

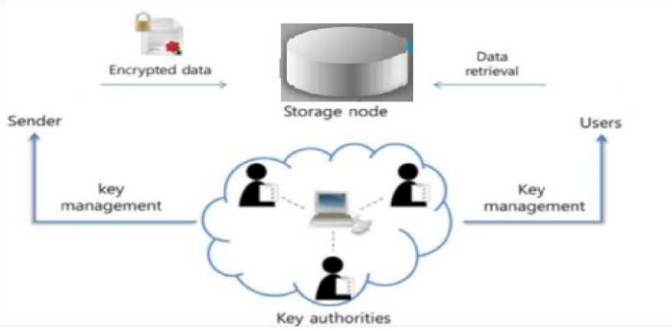

Fig 2. Architecture of the proposed system

4. FEATURES IN PROPOSED SYSTEM

One of the major issues with CPABE is the lack of key management, which goes against the goals of CPABE. This produces a challenge when attempting to revoke and prevent a user from using a key. Additionally, paired with revocation of keys is the fact that in order to replace a key that is no longer valid, users need to go through some sort of renewal process, for either the full key, or only corresponding to specific attributes. So the features we attain from the proposed model are described below.

Key escrow problem

Central authority helps in generation of key for local authority.ie keys are generated by local authorities with the help of master authority. Central authority can decrypt any cipher text in a group. But if master authority key is attacked then entire data can be decrypted. So to solve this encryptor should have some attributes that the decryptor should possess. We propose an Escrow Free Key Issuing Protocol for CP-ABE to resolve escrow problem which utilizes the feature of the data sharing system architecture. Through a secure two-party computation (2PC) protocol among the key generation center and the data storing center with their own master secrets key issuing protocol generates and issues user secret keys. The 2PC protocol prevents them from acquiring any master secret information of each other such that none of them could generate the whole set of user keys on their own. So the users are not necessary to completely belief the KGC and DSC in order to protect their data to be shared. Through the proposed system the data confidentiality and privacy can be cryptographically imposed in opposition to any inquiring KGC or data-storing center (DSC).

Attribute Revocation

The cancellation or revocation of any attribute or single user from an attribute group or set of users will influence all users in that group. i.e. when a user comes to hold or drop an attribute, during a single message transmit or a group message transmit,

then corresponding key should be updated to prevent the user from accessing the previous or subsequent encrypted data for backward or forward secrecy, respectively. In attribute-based encryption, a user who newly holds the attribute that satisfies the access policy might be able to access the previous data encrypted, so he must be disallowed from obtaining the attribute until the data is reencrypted with the newly updated attribute keys by periodic rekeying is called backward secrecy. A revoked user would still be able to access the encrypted data even if he does not hold the attribute any more .This should be prevented and is called forward secrecy. Updation of key is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. When the membership change request for some attribute groups is received it notifies the storage node about the event.

But if a user is withdrawn from some attribute groups he would still be able to decrypt the shared data as long as the other attributes that he holds assures the access policy of the cipher text. One promising way to immediately revoke an attribute of specific users is to reencrypt the ciphertext with each attribute group key and selectively distribute the attribute group key to authorized (non-revoked) users who are qualified with the attribute. This can be done by redefining the master key components for involved attributes by the authority. Corresponding public key components are then updated accordingly. After that data will be encrypted with the new public key. Apparently, user secret keys should be updated accordingly for data access. That is the rekey generation is done by taking as input an attribute set that includes attributes for update and current user key. It outputs the new user key, the new public key and new key for all attributes in attribute union. Reencryption is done with the new public key.

Attribute Renewal

In proposed approach the user is required to give old Secret Key and proof for new attribute value but is not required to give proof for old attributes. This is used by the authority to update the required attribute value, provided if old Secret Key is present and then it gives the new Secret Key. In other words we can say that the old attribute values are collected from old Secret Key and update the required attribute.

Group-oriented attribute based encryption (Bucketization)

We propose and define a variant of ABE know as group based attribute based encryption. In this new notion we divide the users into multiple groups or buckets. Only members from same group can merge their decryption keys but users from different group cannot make it. It means that users from same group are able to cooperate with each other to decrypt a cipher text encrypted under a set of attributes, such that a single user may not have enough attributes to match the attribute set. But users from different groups cannot collude.

This can be achieved in such a way that after dividing all the involved users into multiple “buckets” (say m) of a suitable size, then computes an intermediate key for each bucket by executing the Key Generation algorithm, and then computes the actual group key for all the users by executing the Key Generation algorithm with the intermediate keys as the secrets. Note that the intermediate key generation can be parallelized as each bucket is independent.

5. EXPERIMENTAL SETUP

The parameter which we are going to evaluate in this project is security. Since security is not a measurable field we ensure this by considering the packet drop.

Packet loss/drop

Packet loss/drop is the failure of one or more transmitted packets to reach at their destination. Hence the packet drop rate can be estimated by no of packets drop in simulation time. Here we are comparing the CP-ABE with CP-AUBE. That is, we are comparing the encryption based on security and without security.

Since we are enforcing attribute union based encryption the packet drop attack will be less. We can clearly observe that the proposed model outperforms the other ones in reduced packet drop.

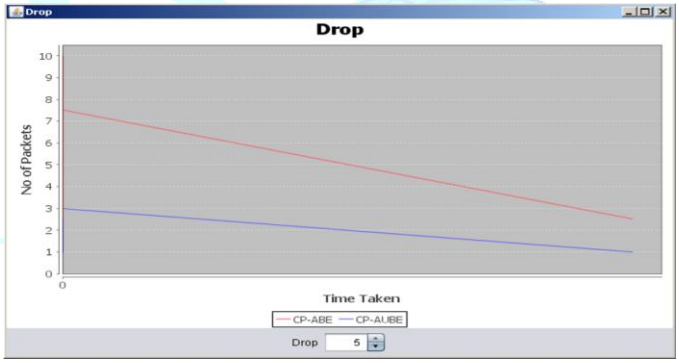

Fig 3. Pack drop rate

6. CONCLUSION AND FUTURE SCOPE

In the disruption tolerant networks the application of access policies and the support of policy update are challenging issues. In this work we proposed a cipher policy attribute based data sharing scheme to levy an elegant data access control by making use of the characteristic of the wireless networks. The proposed system removes key escrow problem during the key generation, where the secret keys are generated via a protected two-party computation (2PC) protocol, which ensures that any inquiring key generation center or datastoring center cannot get the private keys independently. We can do an immediate user revocation on every attribute set at the same time as taking complete advantage of the scalable access control. Also we ensure an efficient attribute renewal, key updation and it also supports group oriented attribute based encryption using the concept of bucketization. As a result, the proposed system achieved more

secure and elegant data access control in the disruption tolerant networks.

The limitation of the approach proposed is its static in nature. Currently the attribute renewal is done by local authority with the permission of central authority. We can make attribute renewal dynamic in future, such that CA can update dynamic attributes. Also currently the request for key and attribute is to be approved by central authority. There are cases where central authority may face network issues. Currently it is handled by introducing a secondary central authority which takes all the functionalities of CA. So in future this is handled more effectively.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, *Member, IEEE, ACM* "Secure Data Retrieval for Decentralized DisruptionTolerant Military Networks", IEEE/ACM transactions on networking, VOL. 22, NO. 1, february 2014 [2] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009. [3] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.

[4] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[5] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated Cipher text -Policy Attribute-Based Encryption and Its Application," Proc. Int"l Workshop Information Security Applications (WISA "09), pp. 309323, 2009.

[6] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Int"l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt "05), pp. 457473, 2005.

[7] J. Bethencourt, A. Sahai, and B. Waters, "Cipher text Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[8] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.

[9] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, pp. 273-285, 2010.