Data Monitor- Data based Access Control Mechanism to Secure the Data Dissemination in the Disruption Tolerant Network

I. Ajitha
PG Scholar
Department of Computer Science Engineering
Ranganathan Engineering College

B. Suganya Devi M.E.,
Assistant Professor
Department of Computer Science Engineering
Ranganathan Engineering College

Abstract

Disruption tolerant networking (DTN) technology is designed to deal with the intermittent connectivity among mobile nodes due to mobility, short range radios or terrain obstacles. Our schemes utilize both query and data replications to enhance the query success rate. Besides designing efficient query and data dissemination schemes, one needs to consider the security aspects since sensitive data should only be accessed by authorized personnel. In this paper, we present a data-centric security solution for an information retrieval system which we design for DTN environments through the Access Control mechanism through Multi Authority specific Attribute based encryption (MA-ABE). We also describe the preliminary prototype that we have built. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the CP-ABE scheme in terms of computational and communication overhead under comparable security levels while providing message and Identity privacy.

Keywords : Access Control Mechanism, Multi Authority, Attribute based Encryption, Data Privacy, Data Retrieval, Disruption Tolerant Networking.

1.Introduction

In Military network, with technology advancement, many computing devices like sensors have wireless interfaces and hence can form ad hoc networks. Wireless adhoc networks allow nodes to communicate with one another without relying on any fixed infrastructure. These rapidly deployable networks are very useful in several scenarios e.g. battlefield operations, disaster relief centres etc. Routing algorithms designed for adhoc networks, e.g. [1], do not work in challenging network scenarios where node mobility, terrain obstacles, limited radio range, etc. often result in frequent network partitions. Recently, some solutions have been proposed to deal with such challenging communication scenarios. For example, disruption tolerant networks (DTN) s [2],[4],[5] are designed to overcome such limitations. Several routing schemes have been proposed for DTNs. Some use history based information to estimate delivery probability of peers and pass the messages to the peer that can best deliver the messages [7], [8]. Such routing schemes rely on the node mobility to deliver packets amidst frequent network partitions using a store and forward approach. Although routing is an important design issue, the ability to access information rapidly is also an important feature that a DTN should provide since the ultimate goal of having such a network is to allow mobile nodes to access information quickly and efficiently. For example, in a battlefield, soldiers need to access relevant information e.g. terrain descriptions, weather, intelligent information, locations of enemy and friendly forces etc. In [3],[9], we have designed two information retrieval schemes that use query/data duplications to enhance the query success rate in DTN environments. Our results show that the scheme that binary spreads replicated data copies and queries can achieve 45% to 460% higher query success ratio when compared to a scheme that does not use any data and query replication. In [3], [9], we do not address any security design. In this paper, we describe a prototype that we have built to provide secure opportunistic data retrievals in challenging network environments. Our prototype system uses a data-centric security solution. In our solution, authorized users derive encryption keys for the data items which they are authorized to publish or access from the access keys they get when they authenticate themselves to a mobile key server. The rest of the paper is organized as follows: In Section 2, our related work existing solutions is discussed. Then, in Section 3, we provide detailed descriptions of the secure data retrieval system that we have built. Next, we present in Section 4 a detailed experimental evaluation of the protocol, we modelled, and finally we conclude our work.

2. Related Work

Attribute Based Encryption

In Disruption tolerant Network, ABE can be classified into key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encrypted only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts which can decrypt and issues the key to each user by embedding the policy into the user’s key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes [4], [7].In ABE , two following solution can be integrated. Attribute Revocation:

It is key revocation mechanisms in CP-ABE and KP-ABE, respectively. Technique can be appended to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [8], [13] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering these as attributes [4], [9]. Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is re-encrypted with the newly updated attribute keys by periodic rekeying (backward secrecy). For example, assume that at time, a cipher text is encrypted with a policy that can be decrypted with a set of attributes (embedded in the user's keys) for users. After time, say, a user newly holds the attribute set. Even if the new user should be disallowed to decrypt the cipher text for the time instance, he can still decrypt the previous cipher text until it is re-encrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). We call this uncontrolled period of time windows of vulnerability. The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the non-revoked users can update their keys. This results in the "1-affects-" problem, which means that the update of a single attribute affects the whole non revoked users who share the attribute [19]. This could be a bottleneck for both the key authority and all no revoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses [4], [14]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead group elements1 additively to the size of the ciphertext and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt et al. [13], where is the maximum size of revoked attributes set2. Decentralized ABE: Huang et al. [9] and Roy et al. [4] proposed decentralized CP-ABE schemes in the multi-authority network environment. They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy.

3. Overview

Access Control Mechanism to Secure the Data Dissemination

In this section, we provide an Access Control Mechanism through multi-authority 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 immediately. Thus, the scalability and security can be enhanced in the proposed scheme. Since the first CP-ABE scheme proposed by Bettencourt et al. [13], dozens of CP-ABE schemes have been proposed [7] .The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bettencourt et al.'s scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Access control Scheme Consist of the Following Operations.

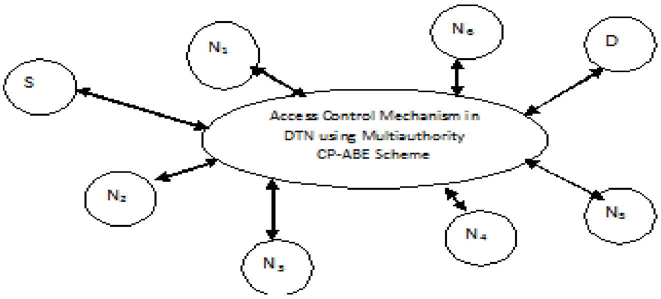
N_1
N_6
D
S
Access Control Mechanism in DTN using Multiauthority CP-ABE Scheme
N_2
N_3
N_4
N_5

Figure 1: Architecture of the Access control Mechanism through CP-ABE

Key Generation: In CP-ABE, user secret key components consist of a single personalized key and multiple attribute keys. The personalized key is uniquely determined for each user to prevent collusion attack among users with different attributes. The proposed key generation protocol is composed of the personal key generation followed by the attribute key generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key escrow problem such that none of the authorities can determine the whole key components of users individually.

Personal Key Generation: The central authority and each local authority are involved in the following protocol by establishing a central authority (CA) for every local authority with personalized and unique secret key to the users which should be consistent for any further attribute additions to the user.

Modelling the Attribute Key Generation:

After setting up the personalized key component, Ai generates attribute keys for a user with a public parameter received from CA. During the key generation phase using the 2PC protocol,

The proposed scheme (especially 2PC protocol) requires messages additively to the key issuing overhead in the previous multi-authority ABE schemes in terms of the communication cost, In terms of the computation cost, each local authority is required to perform two more exponentiation operations.

Data Encryption of Attributes :

When a sender wants to deliver its confidential data, he defines the tree access structure over the universe of attributes, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm chooses a polynomial for each node in the tree. These polynomials are chosen in a top-down manner, starting from the root node. For each node in the tree, the algorithm sets the degree of the polynomial to be one less than the threshold value of that node It is important to note that the sender can define the access policy under attributes of any chosen set of multiple authorities without any restrictions on the logic expressiveness as opposed to the previous multi-authority scheme.

Data Decryption:

When a user receives the cipher text from the storage node, the user decrypts the cipher text with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm a private key, which is associated with a set of attributes, and a node from the tree. It outputs a group element.

Revocation of the Attributes

We observed that it is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs. One promising way to immediately revoke an attribute of specific users is to encrypt 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. Before distributing the cipher text, the storage node receives a set of membership information for each attribute group that appears in the access tree of from the corresponding authorities.

4. Experimental results

In this section, we first analyze and compare the efficiency of the proposed scheme to the previous multi-authority CP-ABE schemes in experimental aspects through NS2 Simulator. 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. In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption.

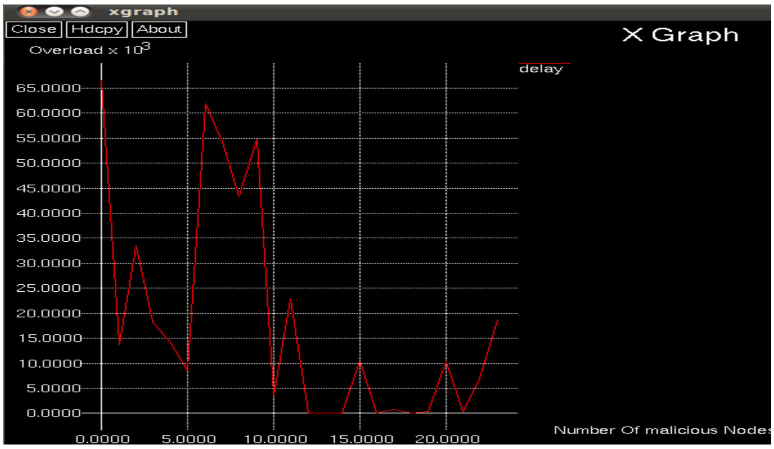

Figure 2: Performance Evaluation of the Proposed Scheme against the Overhead with respect to Malicious Node

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. In Figure 2, the communication cost of the system is predicted against the malicious node propagation in the network.

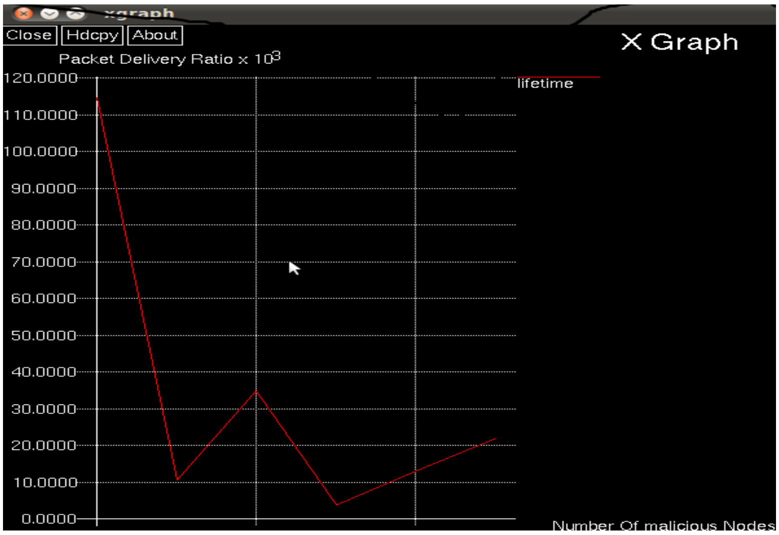

Figure 3: Performance Evaluation of the Proposed System against Packet Delivery Ratio and Malicious Nodes

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 keying messages for no 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.

Data Confidentiality

In our trust model, the multiple key authorities are no longer fully trusted as well as the storage node even if they are honest. Therefore, the plain data to be stored should be kept secret from them as well as from unauthorized users. In Figure 3. We experiment the performance against the data loss due to malicious node, which proves Data confidentiality on the stored data against unauthorized users can be trivially guaranteed. If the set of attributes of a user cannot satisfy the access tree in the cipher text, he cannot recover the desired value.

Backward and Forward Secrecy

When a user comes to hold a set of attributes that satisfy the access policy in the ciphertext at some time instance, the corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key in the cipher text are re-encrypted by the storage node with a random, and the cipher text components corresponding to the attributes are also encrypted with the updated attribute group keys.

5. Conclusion

We have modelled an Access Control Mechanism to secure data dissemination in DTN technologies, DTN 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. Multi authority based CP-ABE for decentralized DTNs has modelled to deny the malicious behaviours where multiple key authorities manage their attributes independently. Finally the key revocation has been done for attribute group with malicious node or attributes. Experimental results demonstrate the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

6.Reference

[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] M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in Proc. IEEE MILCOM, 2006, pp. 1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, “Message ferry route design for sparse ad hoc networks with mobile nodes,” in Proc. ACM MobiHoc, 2006, pp. 37–48.

[4] 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.

[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. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable secure file sharing on untrusted storage,” in Proc. Conf. File Storage Technol., 2003, pp. 29–42.

[7] 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.

[8] 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.

[9] D. Huang and M. Verma, “ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.

[12] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

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

[14] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-based encryption with non-monotonic access structures,” in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 195–203.