International Journal of Scientific Engineering and Innovative Research
Issue : 1 Volume : 1 Year : 2018

A Study on the velocity Control Mechanism in the Disruption Tolerant Military Network

DivyaShree .P
PG Scholar
Department Of Information Technology
SNS College of Technology

S. Sugashini
Assistant Professor
Department of Information Technology
SNS College of Technology

Abstract

Disruption tolerant networking (DTN) technology is designed to deal with the intermittent connectivity among mobile nodes due to mobility, intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios and short range radios or terrain obstacles. DTN network become efficient Communication technology for critical network environment. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. In this survey, we analyse the Cipher text-policy attribute-based encryption (CP-ABE) which 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. A secure data retrieval scheme using CP-ABE for decentralized DTNs has been used as current research with multiple key authorities manages 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: Disruption Tolerant Network, Access Control Mechanism, Attribute Based Encryption, Access Revocation.

1. Introduction

Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each there in these extreme networking environments [1]–[3]. 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 [4] and Chuah [5] 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 [6], [7]. 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 The concept of attribute-based encryption (ABE) [11]–[14] is a promising approach that fulfils 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 encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the cipher text [13]. 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 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 attribute 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. . The remainder of this paper is organized as follows: In Section 2, we describe the related anonymous routing protocols, In Section 3, performance of ABE algorithm and revocation strategies to control access to DTN. In Section 4, the conclusion and future work are given.

2. Related Work

Attribute Based Encryption

Attribute Base Encryption is defined as access control mechanism. It is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes. In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.ABE can be further classified in two techniques named as key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE).

Key policy –Attribute Based Encryptor

It is modelled as the encryptor 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 he can decrypt and issues the key to each user by embedding the policy into the user's key.

Cipher Text – Attribute based Encryptor

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 as follows :

1) Attribute Revocation:

It is a key revocation mechanism in CP-ABE and KP-ABE, respectively. Their solutions are to append 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 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. 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). The immediate key revocation can be done by revoking users using ABE that supports negative clauses. 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.

2) Key Escrow: Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information [11], [13], [14]. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time.

3. Overview of Access Security Models in DTN

In this section we analyse the different proposal related to the securing of the data retrieval in the DTN, as follows

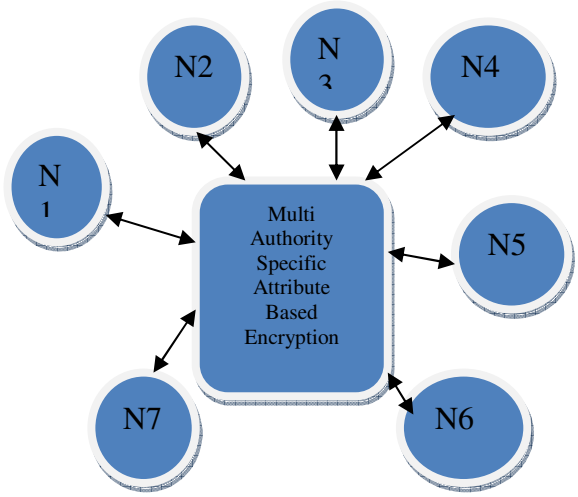

Figure 1: Secured Data Retrieval in DTN

Decentralizing Attribute-Based Encryption

We analyse a Multi-Authority Attribute-Based Encryption (ABE) system. In proposed system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority "tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

Identity-based Encryption with Efficient Revocation

Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). Any setting, PKI- or identity-based, must provide a means to revoke users from the system. Efficient revocation is a well-studied problem in the traditional PKI setting. However in the setting of IBE, there has been little work on studying the revocation mechanisms. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority. We note that this solution does not scale well – as the number of users increases, the work on key updates becomes a bottleneck. We analyse an IBE scheme that significantly improves key-update efficiency on the side of the trusted party (from linear to logarithmic in the number of users), while staying efficient for the users.

Provably secure and efficient bounded cipher text policy attribute based encryption

In a cipher text-policy attribute-based encryption (CP-ABE) scheme, the data is encrypted under an access policy defined by a user who encrypts the data and a user secret key is associated with a set of attributes which identify the user. A user can decrypt the cipher text if and only if his attributes satisfy

the access policy. In CP-ABE, since the user enforces the access policy at the encryption phase, the policy moves with the encrypted data. This is important for data storage servers where data confidentiality must be preserved even if the server is compromised or un-trusted. In this paper, we provide an efficient CP-ABE scheme which can express any access policy represented by a formula involving $\wedge$ and $\vee$ Boolean operators. The scheme is secure under Decision Bilinear DiffieHellman assumption (DBDH). Furthermore, we extend the expressivity of the scheme by including of (threshold) operator in addition to $\wedge$ and $\vee$ operators.

Randomizable proofs and delegatable anonymous credentials

We analyse an efficient delegatable anonymous credentials system. Users can anonymously and unlinkably obtain credentials from any authority, delegate their credentials to other users, and prove possession of a credential L levels away from a given authority. The size of the proof (and time to compute it) is O (Lk), where k is the security parameter. The only other construction of delegatable anonymous credentials relies on general non-interactive proofs for NP-complete languages of size kΩ (2L). We revise the entire approach to constructing anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block.

Node density-based adaptive routing scheme for disruption tolerant networks

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. Hence, routing mechanisms that can withstand disruptions need to he designed. A store-and-forward approach has been proposed for disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks e.g. the 2-hop relay approach, delivery probability based routing, and message ferrying. In our earlier analysis, we have determined a combined multihop and message ferrying approach in disruption tolerant networks. In that paper, we assume that a special node is designated to be a message ferry. A more flexible approach is to let regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, in this survey, we design a node-density based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications.

Removing escrow from identity-based encryption

Key escrow is inherent in identity-based encryption (IBE). A curious key generation center (KGC) can simply generate the user's private key to decrypt a cipher text. All existing pairing-based IBE schemes without random oracles, whether receipt-anonymous or not, do not achieve KGC onewayness, a weaker notion of ACI − KGC. In view of this, we first show how to equip an IBE scheme by Gentry with ACI − KGC. Second, we propose a new system architecture with an anonymous private key generation protocol such that the KGC can issue a private key to an authenticated user without knowing the list of user's identities. This also better matches the practice that authentication should be done with the local registration authorities instead of the KGC.

4. 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 survey, 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.

5. 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 cipher text 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 cipher text-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, "Cipher text-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.

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