International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 10, Volume 2 (October 2015) www.ijirae.com

Review On Colloborative Approach For Securing Data Retrieval For Decentralized Distruption Tolerant Military Network.

Ruchi Rajkumar Bajpai
Department of Computer Science & Engineering,
Rajiv Gandhi College of Engineering,
Research &Technology, Chandrapur-442401

Prof. P.K. Kulkarni
Department of Information Technology,
Rajiv Gandhi College of Engineering
Research &Technology, Chandrapur-442401

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— ABE, DTN, CP-ABE, Attribute revocation, Key escrow, Decentralized ABE, wireless networks.

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-nodes to communicate with each other in these extreme networking environments. 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.DTN architecture may be referred as where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

II. BRIEF LITERATURE SURVEY

ABE comes in two flavors called key-policy

A. ABE (KP-ABE) and
B. Cipher text-policy ABE (CP-ABE).

I. KP-ABE

In KP-ABE, 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 ciphertexts he can decrypt and issues the key to each user by embedding the policy into the user's key.

II. Cipher text-Policy ABE (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.

A. Attribute Revocation:

Solutions proposed 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. 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 nonrevoked 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. This could be a bottleneck for both the key authority and all nonrevoked users. 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. This scheme will pose overhead group elements1 additively to the size of the cipher text and multiplicatively to the size of private key over the original CP-ABE scheme of Bethencourt et al., where is the maximum size of revoked attributes set . Golle et al. also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a cipher text is exactly half of the universe size.

B. 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. 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.

Chase et al. presented a distributed KP-ABE scheme that solves the key escrow problem in a multiauthority system. In this approach, all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases components besides the attributes keys, where is the number of authorities in the system.

C. Decentralized ABE:

Huang et al. and Roy et al. proposed decentralized CP-ABE schemes in the multiauthority 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. For example, when a commander encrypts a secret mission to soldiers under the policy ("Battalion 1" AND ("Region 2" OR 'Region 3")), it cannot be expressed when each "Region" attribute is managed by different authorities, since simply multiencrypting approaches can by no means express any general " -out-of- " logics (e.g., OR, that is 1-out-of-). For example, let be the key authorities, and be attributes sets they independently manage, respectively. Then, the only access policy expressed with is, which can be achieved by encrypting a message with by , and then encrypting the resulting cipher text with by (where is the cipher text encrypted under), and then encrypting resulting cipher text with by , and so on, until this multiencryption generates the final cipher text . Thus, the access logic should be only AND, and they require iterative encryption operations where is the number of attribute authorities. Therefore, they are somewhat restricted in terms of expressiveness of the access policy and require computation and storage costs.

Chase and Lewko et al. proposed multiauthority KP-ABE and CP-ABE schemes, respectively. However, their schemes also suffer from the key escrow problem like the prior decentralized schemes.

III. PROBLEM FORMULATION

Storage nodes in DTNs were used, 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. Attribute-based encryption (ABE) 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 cipher texts.

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.

The problem of applying the ABE to DTNs introduces several security and privacy challenges. 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.

IV. OBJECTIVE

A. Improved security in storage node for secure and efficient data retrieval.
B. Updating the security policies does not affect the users.
C. The confidentiality of the data is improved so that the stored data is guaranteed under hostile region.
D. The feature of multiauthority CP-ABE scheme gets enhanced and the problems in this scheme are reduced.
E. The leased time for retrieving data can be extended if the user was not able to retrieve the data in the allotted time.

V. PROPOSED METHODOLOGY

The main contributions of this paper are as follows:

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, encryptors 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.

VI. CONCLUSIONS

Thus we have presented collaborative approach for securing decentralized DTN for military network that comprehensively address various practical limitations of the earlier approaches.

We propose a method in which the access policy need not be sent along with the cipher text, by which we are able to preserve the privacy of the encryptor. This techniques encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks.

ACKNOWLEDGMENT

We would like to thank Department of Computer Science & Engineering, RCERT Chandrapur for providing infrastructure and guidance to understand Security of Decentralized Distruption Tolerant Military Network.

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]. 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.ACMn Mobi Hoc, 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,” LehighCSE Tech. Rep., 2009.
[5]. M. Chuah and P. Yang, “Performance evaluation of content-basedinformation 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]. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM “Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks”- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.
[9]. 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
[10]. 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.
[11]. A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” Cryptology ePrint Archive: Rep. 2010/351, 2010.
[12]. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc. Eurocrypt, 2005, pp. 457–473.
[13]. 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.
[14]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” in Proc. IEEE Symp. Security Privacy, 2007, pp. 321– 334
[15]. 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.
[16]. S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in Proc. ASIACCS, 2010, pp.261–270

[17]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proc. ACM Conf . Comput. Commune. Security, 2008 , pp. 417–426
[18]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 99–112.
[19]. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput. Surv., vol. 35, no. 3, pp. 309–329, 2003.
[20]. S. Mittra, "Iolus: A framework for scalable secure multicasting," in Proc. ACM SIGCOMM, 1997, pp. 277–288.
[21]. P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in Proc. Symp. Identity Trust Internet, 2008, pp. 26–35
[22]. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465

