International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

HUMANIZING PRIVACY AND SECURITY BASED DATA RETRIEVAL FOR DDTN NETWORKS

G.Jayahari Prabhu
II M.E Communication Systems
PSN College of Engineering and Technology, Tirunelveli
jayahariprabhu@gmail .com

S.Manikandan
Asst Professor, Dept of ECE
PSN College of Engineering andTechnology, Tirunelveli
sl.manikandan@gmail.com

Abstract— Disruption-tolerant network (DTN) technologies are becoming flourishing solutions that allow wireless devices carried by soldiers to communicate with each other and access the secret information or command dependably by exploit external storage nodes. In this paper, propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. Here demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Index Terms— Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure Data retrieval.

1 INTRODUCTION

In a lot of 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-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other 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. 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. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should 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 changed (e.g., the attribute representing current location of moving soldiers) [4], [8], [9]. We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN [10].

The concept of attribute-based encryption (ABE) [11]–[14] is a promising approach that fulfills the requirements for secure data retrieval in DTNs.

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 ciphertext 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 singlemaster secret is the basicmethod 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.

2 NETWORK ARCHITECTURE OF DDTN

In this section, we describe the DTN architecture and define the security model.

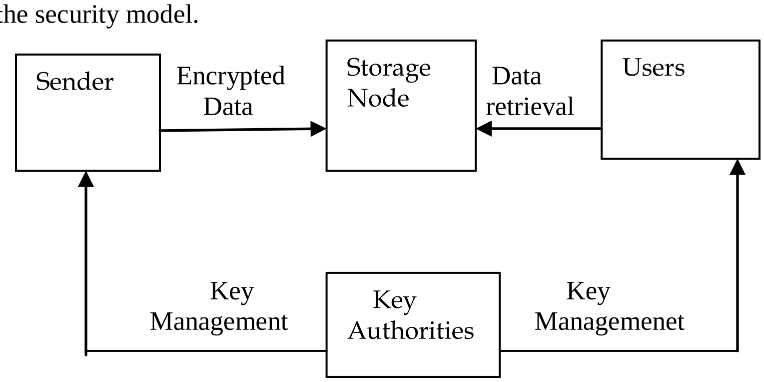

Fig 1: Architecture of secure data retrieval in a DTN networks

International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities.

   Assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.
2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static [4], [5]. Similar to the previous schemes, we also assume the storage node to be semitrusted that is honest-but-curious.
3) Sender: 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.
4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the ciphertext and obtain the data.

3 EXPERIMENTAL EVALUTION

We first provide a formal definition for access structure recapitulating the definitions in [12] and [13]. Then, we will briefly review the necessary facts about the bilinear map and its security assumption.

Access Structure: Let $\{P_1, P_2, \ldots, P_n\}$ be a set of parties. A collection $\mathbb{A} \subseteq 2^{\{P1, P2, \ldots, Pn\}}$ is monotone if $\forall$ B, C: If $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbb{A}$ of nonempty subsets of $\{P_1, P_2, \ldots, P_n\}$, i.e., $\mathbb{A} \subseteq 2^{\{P1, P2, \ldots, Pn\}} \setminus \{\emptyset\}$. The sets $\mathbb{A}$ in are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

In the proposed scheme, the role of the parties is taken by the Attributes. Thus, the access structure $\mathbb{A}$ will contain the authorized sets of attributes. From now on, by an access structure, we mean a monotone access structure.

Definitions:

$x \in_R S$ denotes the operation of picking an element x at random and uniformly from a finite set S. For a probabilistic algorithm$\mathcal{B}$, $x \overset{\$}{\leftarrow} \mathcal{B}$ assigns the output $\mathcal{B}$ of to the variable$x$. 1^{λ} Denotes a string of λ ones, if $\lambda \in \mathbb{N}$. A function $\varepsilon: \mathbb{N} \to \mathbb{R}$ is negligible (negl (k)) if for every constant $c \geq 0$ there exists k_c such that $\epsilon(k) < k^{-c}$ for all $k > k_c$.

Let $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$ be the universe of users. Let CA be the central authority, and $\mathcal{A} = \{A_1, \ldots, A_n\}$ be the universe of local authorities. Let $\mathcal{L} = \{\lambda_1, \ldots, \lambda_p\}$ be the universe of descriptive attributes in the system. Let A_i $(\mathcal{L})$ be the set of attributes managed byA_i (we assume each local authority manages a disjoint set of attributes such that $A_i(\mathcal{L}) \cap A_j(\mathcal{L}) = \emptyset$ for $i \neq j$).
Let $G_i \subset \mathcal{U}$ be a set of users that hold the attributeλ_i, which is referred to as an attribute group.

4 PROPOSED SCHEME FOR DDTN NETWORKS

In this section, this paperprovide a multiauthority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local auhority issues partial personalized and attribute key components to a ser 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 Bethencourt *et al.* [13], dozens of CP-ABE schemes have been proposed [7]

1) Description: Let $\mathcal{T}$ be a tree representing an access structure. Each nonleaf node of the tree represents a threshold gate. If $num_x$is the number of children of a node x and k_x is its threshold value, then $0 \leq k_x \leq num_x$. Each leaf node x of the tree is described by an attribute and a threshold value $k_x = 1$. λ_x denotes the attribute associated with the leaf node x in the tree. $\mathcal{P}(x)$ represents the parent of the node x in the tree. The children of every node are numbered from 1 to num. The function intex(x) returns such a number associated with the node x. The index values are uniquely assigned to nodes in the access structure for a given key in an illogical manner.

2) 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.

3) Data Encryption: When a sender wants to deliver its confidential data M, he defines the tree access structure $\mathcal{T}$ over the universe of attributes$\mathcal{L}$, encrypts the data under $\mathcal{T}$ to enforce attribute-based access control on the data, and stores it into the storage node.

The encryption algorithm chooses a polynomial q_x for each node x in the tree $\mathcal{T}$. These polynomials are chosen in a topdown manner, starting from the root node R.

For each node x in the tree $\mathcal{T}$, the algorithmsets the degree of d_x the polynomial q_x to be one less than the threshold value k_x of that node, that is, $d_x = k_x - 1$. For the root node R, it chooses a random $s \in \mathbb{Z}_p^*$ and sets $q_R(0) = s$. Then, it sets d_R other points of the polynomial q_R randomly to define it completely. For any other node x, it sets $q_x(0) = q_{p(x)}(index(x))$ and chooses d_x other points randomly to completely define q_x.

Let Y be the set of leaf nodes in the access tree. To encrypt a message $M \in \mathbb{G}_1$ under the tree access structure $\mathcal{T}$, it constructs a ciphertext using public keys of each authority as

$$CT = \left(\mathcal{T}, \tilde{C} = Me(g,g)^{(\alpha_1+\cdots+\alpha_m)s}, C = h^s, \forall y \in Y : C_y = g^{q_y(0)}, C_y' = H(\curlywedge_y)^{q_y(0)}\right)$$

S Where $\tilde{C}$ can be computed as $\tilde{C} = M.\left(PK_{A_1} \times \ldots \times PK_{A_m}\right)^s = Me(g,g)^{(\alpha_1+\cdots+\alpha_m)s}$.

After the construction of CT, the sender stores it to the storage node securely. On receiving any data request query from a user, the storage node responds with CT to the user.

4) Data Decryption: When a user receives the ciphertext CT from the storage node, the user decrypts the ciphertext with its secret key. The algorithm performs in a recursive way. We first define a recursive algorithm that DecryptNode(CT, SK, x) takes as inputs a ciphertext CT, a private key SK, which is associated with a set $\wedge$ of attributes, and a node x from the tree $\mathcal{T}$. It outputs a group element of $\mathbb{G}$ or $\perp$.

Without loss of generality, we suppose that a user u_t performs the decryption algorithm. If x is a leaf node, then define as follows. If $\curlywedge_x \in \wedge$, then

DecryptNode (CT, SK, x)

$$= \frac{e(D_x, C_x)}{e(D_x', C_x')}$$

$$= \frac{e\left(g^{r_t}.H(\curlywedge_x)^{r_x}, g^{q_x(0)}\right)}{e\left(g^{r_x}, H(\curlywedge_x)^{q_x(0)}\right)}$$

$$= \frac{e\left(g^{r_t}, g^{q_x(0)}\right).e\left(H(\curlywedge_x)^{r_x}, g^{q_x(0)}\right)}{e\left(g^{r_x}, H(\curlywedge_x)^{q_x(0)}\right)}$$

$$= e(g,g)^{r_t q_x(0)}.$$

Attribute based technique

ABE comes in two flavors called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a ciphertext 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. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set.

1) Attribute Revocation: Bethencourt *et al.* [13] and Boldyreva *et al.* [14] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively.

For example, assume that at time , a ciphertext is encrypted with a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with . After time , say , a user newly holds the attribute set . Even if the new user should be disallowed to decrypt the ciphertext for the time instance , he can still decrypt the previous ciphertext until it is reencrypted with the newly updated attribute keys.

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]- [14] . Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time.

3) Decentralized ABE: They achieved a combined access policy over the attributes issued from different authorities by simply encrypting data multiple times.

B. Contribution

In this paper, we propose an attribute-based secure data etrieval scheme using CP-ABE for decentralized DTNs. The pro osed 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. 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.

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

5 PERFORMANCE EVALUATION

A. Efficiency

In the proposed scheme, the logic can be very expressive as in the single authority system like BSW [13] such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV [9] and RC [4] schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done in an immediate way as opposed to BSW.

system	Ciphertext size	Rekeying message	Private key size	Pulic key size
HSW[13]	$(2t + 1)C_0 + C_1 + C_{\mathcal{T}}$	$l(2k+1)C_0$	$(2k + 1)C_0$	$C_0 + C_1$
HV[9]	$(2t + m)C_0 + mC_1 + C_{\mathcal{T}}$	$l(2k+1)C_0$	$(2k+m)C_0$	$mC_0 + mC_1$
RC[4]	$(2t + 3r + m)C_0 + mC_1 + C_{\mathcal{T}}$	0	$(3k+2m)C_0$	$m(t + 4)C_0 + mC_1$
Proposed	$(2t + 1)C_0 + C_1 + C_{\mathcal{T}}$	$(n - l)log\frac{n}{n-l}C_p$	$(2k+1)C_0+lognC_k$	$C_0 + mC_1$

Table1: Effciency Analysis

C_0: bit size of an element in $\mathbb{G}_0$, C_1: bit size of an element in $\mathbb{G}_1$, C_p: bit size of an element in $\mathbb{Z}_p^*$, C_k: bit size of a KEK, $C_{\mathcal{T}}$: bit size of an access tree $\mathcal{T}$ in the ciphertext, r: the number of revoked users, l: the number of users in an attribute

B. *Simulation*

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption.

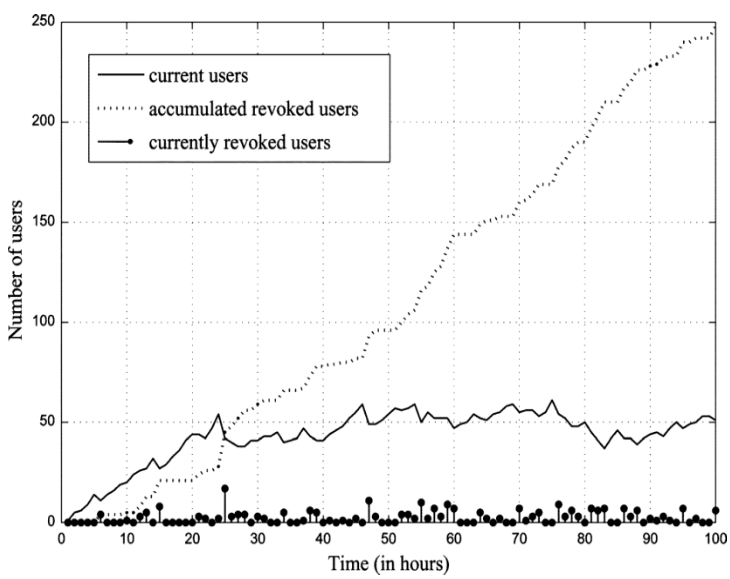

Fig 2: Number of Users in an Attribute group

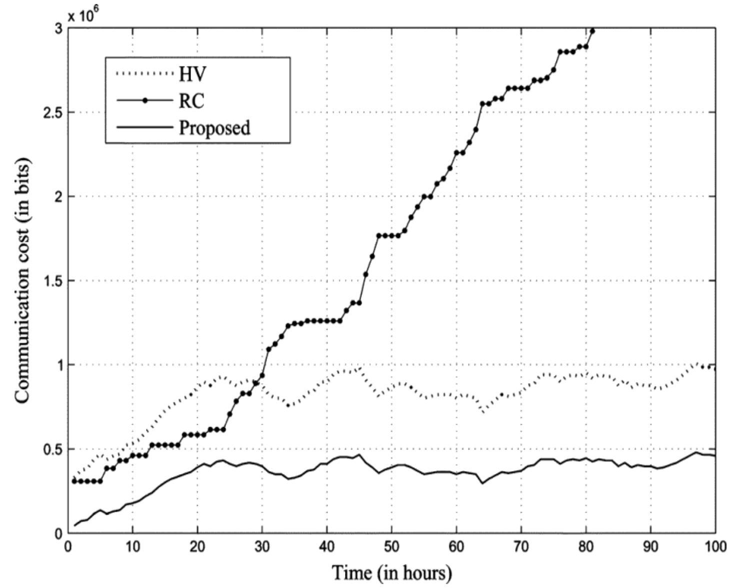

Fig 3:communication cost in the multiauthority system

If 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. We set the interarrival time between users as 20 min and the average membership duration time as 20 h . Fig. 2 represents the number of current users and revoked users in an attribute group during 100 h. Fig. 3 shows the total communication cost that the sender or the storage node needs to send on a membership change in each multiauthority CP-ABE scheme. It includes the ciphertext and rekeying messages for nonrevoked users. It is measured in bits. In this simulation, the total number of users in the network is10 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.

6 CONCLUSION

The secured & efficient data retrieval method using cipher policy –attribute based encryption for decentralized DTNs are proposed in this work.Multiple key authorities are handle their attribute independently.the detailed demonstration is available for how to apply the proposed mechanism to steadily and capably manage the secret data isolated in the disruption tolerant military networks

ACKNOWLEDGMENT

The authors would like to thank the reviewers for their constructive comments.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "maxpop Routing for vehicle based disruption tolerant network," in Proc.IEEE INFOCOM, 2013, pp. 1–11.

[2] M. Chuah and P. Yang, "Node density-based adaptive routing Scheme for disruption tolerant networks," in *Proc. IEEE MI COM*, 2006, pp. 1–6.

[3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry rou design for sparse ad hoc networks with mobile nodes," in Proc. ACM MobiHoc, 2010, pp. 37–48.

[4] 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.

[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., 2009, 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, 2009, 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 attributebased 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.