IWNEST PUBLISHER

Journal of Industrial Engineering Research

(ISSN: 2077-4559)

Journal home page: http://www.iwnest.com/AACE/

Cipher text Policy-Attribute Based Encryption for Data Retrieval in Disruption-Tolerant Networks

[1]C. Balakrishnan, [2]P.Divya and [3]P. M. Blessey

[1]Assistant Professor S.A Engineering College Chennai, Tamil Nadu
[2]PG Scholar S.A Engineering College Chennai, Tamil Nadu
[3]PG Scholar S.A Engineering College Chennai, Tamil Nadu

ARTICLE INFO

Article history:
Received 22 February 2015
Accepted 20 March 2015
Available online 23 April 2015

Keywords:
Attribute-based encryption (ABE), Disruption-tolerant network (DTN), Revocation key, Key authority, Secure data retrieval.

ABSTRACT

A military environment such as a battlefield or a hostile region is likely to suffer from temporary disconnections like jamming, environmental factors, and mobility. Disruption tolerant network [1] are the successful solution that allow wireless devices carried by soldiers to communicate with each other and access the confidential information by exploration storage nodes includes authorization policy or by updating policy .The policies include cipher- text policy attribute based encryption enables encryptors 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 . The problem of applying Cp-Abe [2] in DTN includes attribute revocation, key escrow, and coordination of attribute. In proposed system, immediately enhances backward/forward secrecy, escrows-free key issuing protocol and monotone access structure for security and efficient management in confidential data.

To Cite This Article: C. Balakrishnan, P. Divya and P.M. Blessey., Cipher text Policy-Attribute Based Encryption for Data Retrieval in Disruption-Tolerant Networks. **J. Ind. Eng. Res.,** *1(4), 79-85, 2015*

INTRODUCTION

A military network, suffer from major obstacles like disconnections of wireless devices carried by soldiers to communicate with one another, sparsity of mobile nodes and energy resources. A disruption-tolerant network [1] (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact and become solutions for mobile nodes to communicate with each other in these extreme military environments. The messages between node to node may needed to wait in intermediate node for certain period of time when there is no end-to-end connection between them.

Roy [4] and Chuah [5] introduced storage nodes between the mobile nodes where data is stored or retrieved quickly and efficiently within some authorized nodes. The authorization for nodes is provided by access control policy. The data access policies are defined over user attributes or roles, which are controlled by the key authorities. The Disruption tolerant networks (DTN) architecture is used when multiple authorities manage their own dynamic attribute keys independent as a decentralized DTN [6]. For example: the attribute representing current location of moving soldiers in a battlefield or hostile region.

Application such as space environment and terrestrial environment in which terrestrial environment mainly concerned with Intermittently Connected Networks(ICNs) and frequency partitions(FPs), where ICNs doesn't prevent communication between the disconnected areas and FPs doesn't allow for resource allocation. The terrestrial environment of DTN is envisioned for Under Water Networks (UMNs), Pocket Switched Networks (PSNs), Vehicular Adhoc NETworks (VANETs) [5], and Airborne Networks (ANs).

UMNs are deployed to perform collaborative monitoring tasks over an oceanographic area. The characteristics of UMNs are transmission loss, noise, multipath, high delay and delay variance

PSN is a new communication paradigm for mobile devices. It takes advantage of every communication opportunity, and the physical mobility of the devices, in order to transport data to destinations.

VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

Corresponding Author: C. Balakrishnan, Assistant Professor S.A Engineering College Chennai, Tamil Nadu
E-mail: balakrishnan@saec.ac.in

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 79-85

ANs are proposed network in which all nodes would be located in aircraft. The network is intended for use in aviation communications, navigation, and surveillance (CNS) and would also be useful to businesses, private Internet users, and government agencies, especially the military.

The attribute-based encryption is a promising approach for encryption and decryption using public key encryption (PKE), Identity based encryption (IDE), Fuzzy identity based encryption (Fuzzy-IDE), Cipher-text policy or key policy attribute based encryption(CP-ABE or KP-ABE) [2]. The concept of attribute-based encryption (ABE) [11]–[14] provides access policies and described attributes among private keys and Cipher text. The major difference between CP-ABE and KP-ABE in Cipher text–policy ABE, access policy is associated in the Cipher text and in key-policy ABE access policy is associated with the private key.

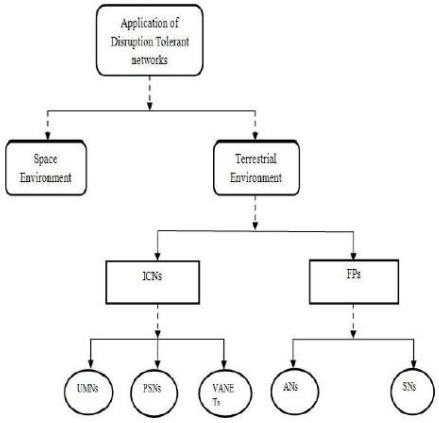

Fig. 1: Architecture of DTN.

II. *Related Work:*

A. Cipher text policy-Attribute based encryption:

CP-ABE [4] is a type of identity-based encryption [11] with one public key and master private key used to make more restricted private keys but very expressive rules employs decryption of private keys for which cipher texts private keys have "attributes" or labels and decryption policies. For working of cp-abe [14], list the parameters that have been configured such as users U = {u1, u2, …..,un} attributes A = {a1, a2,……, ak} and random subset of attributes have been distributed to each user D = {d1, d2,….., dx} where D Є A. Each user encrypt the file in a access tree T structure in which consider each leaf nodes are attributes in A and none leaf nodes is a gate node within the threshold value. The threshold ranges from kx, $0 \leq kx \leq$ numx where numx is the number of children for node x. The condition specification are if the node is an AND kx = numx and so if the node is an OR kx = 1. The Cp-abe functions included are

Setup: Choose a bilinear B0 of prime Order a, generator b and random exponents α, β Є za generates PUK = B0, a, b = aβ, c= a1/β, e (a, a)α and its master key is (β, aα)

Encrypt (PUK, Me, T): Me is the message to be encrypted using T is the tree access structure for which choose polynomial bx for each node x in T including the leaves and also order the polynomial bx is kx – 1 where kx is the threshold of node x. For the root R choose bR(0) = s where s is a random number Є za and choose random points to construct the polynomial if other nodes are chosen then construct bx(0) = bparent(x)(index(x)) construct CT = (T, $\hat{C}$ = Me e(a,a)αs, C = hs, y Є Y : Cy = bqy(0), C'y = H(att(y))qy(0)) where Y is the set of the leaf nodes H is a hash function defined as a random oracle defined as H : {0, 1}* → B0

Key generation (MK, S): In this S is a list of attributes associated with the private key now choose r Є Zp and rj Є Zp for each attribute j Є S, the generated key is SK = (D = b(α+r)/β, j Є S : Dj = br.H(j)rj, D'j = brj)

Decrypt (CT, SK, x): $e(Di,Cx)e(D'i,c'x)/$, this function is a recursive, starting from the root node of the tree until the leaves only if the attribute satisfies the tree then the root will be satisfied. Finally the encrypted message Me is being decrypted as Md.

B. Key policy attribute based encryption:

In kp-abe, cipher texts are labeled with a set of attributes and private keys are associated with access structures that control which cipher text a user is able to decrypt. In this, attribute sets are used to generate cipher texts and private keys are associated with access structures that specify which cipher texts the user will use to decrypt. Consider a set of users U = {U1, U2, . . . ,Un}. A selection of nodes A ⊆ 2 U is known to be monotone if, for all B, C, if B ∈ A and B ⊆ C, then C ∈ A. An access structure (resp., monotonic access structure) is a gathering (resp., monotone collection) A ⊆ 2 P \ {∅}. The sets in A are called the authenticated sets, and the sets not in A are called the unauthenticated sets. The Kp-abe functions included are

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 79-85

Setup: This setup attribute is used to set attributes for users it uses randomized algorithm that takes no input but only its security parameter. It describes a bilinear group B0 of prime order a with a generator b where these parameters are used to form a bilinear map e: B1 × B1 → B2. Each user are determined using the public key and master key these are denoted as attribute U = {1, 2… N}, public key PK = (Y, T1, T2…TN) and master key = (y, t1, t2….tN) where Ti Є Bi and ti Є Zp for all attributes I, 1 ≤ i≤ N and y Є B2 is another public key component.

Encryption: It takes an input of message M, the public key PK, and a set of attributes I and produces output as cipher text E. It has contains some format:

E = (I, Ĕ, {Ei Є I}) where Ĕ = MYs, Ei = Tsi and s is randomly selected from Zp.

Secret key generation: It takes access tree T, the master key MK, and the public key k as input and produces output as user secret key SK= {ski}i Є L where L is denoted as the set of attributes associated to leaf nodes of T and ski = bpi(0)/ti.

Decryption: It takes cipher text E, the user's secret key SK and the public key PK finally it produces output as the message M only if I satisfies T.

III. Concept:

The problem of introducing ABE in DTN resembles in authorization and confidential problems. In which some users may switch their correlated attributes at some point (for example, user changing their location from one region to another region), or some users secret key may be known, key revocation (or update). Nevertheless, this problem is even more problematic, in ABE schemes, since each attribute is shared by multiple users due to this, any single user in an attribute group would affect the other users in the same group. For example, in an attribute group any user joins or leaves, the attribute key generated by key authority

An important challenge in ABE is key escrow in which the key authority has the privilege to generate private keys for the users using the authority's master secret keys to users for specific set of at- tributes. Every key authority has the power to decrypt every cipher text of the specific user by creating their particular attribute key due of this security problem arises (i.e.) any key authority is captured by opponent when deployed in the hostile environments or in the battlefield, this leads to data confidentiality and any secret element is handed over to the adversaries, this leads to data integrity or availability. It is an inherent issues even multiple security systems but it uses the asymmetric encryption system to escrows in the single-authority or multiple-authority CP-ABE. This is referenced as open pivotal problem for the military environment.

The final challenge in ABE is the coordination of attributes which are issued from multiple authorities in the attribute group. Even though multiple authorities generates and distributes attribute keys to users separately with their own master secrets, it is found to be difficult to define fine-grained(keen) [7] access policies over attributes provided from multiple authorities. For example, suppose that attributes "user 1" and "region 1" are controlled by the key authority A, and "user 2" and "region 2" are controlled by the key authority B. Then, it becomes difficult to produce an fine grained access policy [7] even it uses Boolean functions. OR Boolean logic in between the attributes generated from different authorities cannot be determined because the different authorities create their own attribute keys using their own independent and individual master secret keys. Therefore, "-out-of-" logic, cannot be expressed in the schemes.

1) Attribute Revocation:

The solutions for the attribute revocation [10] are to specify and register an expiration date (or time) to each users in the attribute group and sends a unique set of keys to authorized users after the expiry date. This comes out with [8], [10], have two main issues.

The first problem in the attribute revocation is the security degradation in order to prevent backward and forward secrecy of the users. It is an included part that any user such as soldier may change their position or location frequently [4], [9]. After that, a user who newly join in the group must able to gain the encrypted data before he gets the attribute until the data is decrypted with the newly revocated attribute keys by frequent rekeying (backward secrecy) procedure. For example, assume that a user generates cipher text is encrypted with some policy that can be decrypted with attributes set at some time or period. After that time, a newly joined user in an attribute group handles that particular set of attribute. Even though a new user doesn't have privilege to decrypt the cipher text for that instance of time, but that new user still have privilege to decrypt the previous cipher text until the attribute is reencrypted with the newly created attribute keys. Next, an updated user would still have the access to encrypted data even if he does not handle the attribute until the next expiration time are defined as forward secrecy. For example, if a user leaves the attribute group at time, he have the privilege to decrypt the cipher text of the previous time instance until the user's key is expired and the cipher text is reencrypted with the newly revocated key that an user cannot access it. This type of problems leads to windows of vulnerability to the opponent.

Another problem in the attribute revocation is the scalability problem. The key authority frequently declares a key revocated material by unicast at each time period so all other users who are not updated can update their

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 79-85

keys. This is concluded in the "1-affects-n" problem, means that revocation of a one user affects the entire non-updated users. This results in bottleneck problem for both the key authority and all non-revoked users. The immediate key revocation can be done by AND (where each is considered as an attribute here). But, this lacks efficiency performance. This becomes overhead for group elements (i.e.) addition to the size of the cipher text and multiplication to the size of private key over the original CP-ABE process

2) Key Escrow:

Most of the previous ABE schemes are constructed with single trusted authority which has the privilege to generate the entire asymmetric keys of users with its master secret information. Since it is inherent such, the key authority can decrypt every cipher text generated at any time. The paper [15] represented a distributed KP-ABE scheme that handles the key escrow problem in a multiauthority system. In this approach, all attribute authorities are involved in the key generation protocol in a distributed way so that attribute authorities notable to send the data and link multiple attribute sets gathered to the same user. The main disadvantage of this approach is the performance degradation. Since it is decentralized authority with master secret information, should communicate with each other in the system to produce a user's secret key. The outcome is O(N2) communication overhead.

3) Decentralized ABE:

The papers [9] and [4] proposed decentralized CP-ABE schemes in the network environment. They obtain a gathered access policy over the users generated from different authorities by encrypting the data many times. The disadvantages are efficiency and expressiveness of access policy.

IV. *Network architecture:*

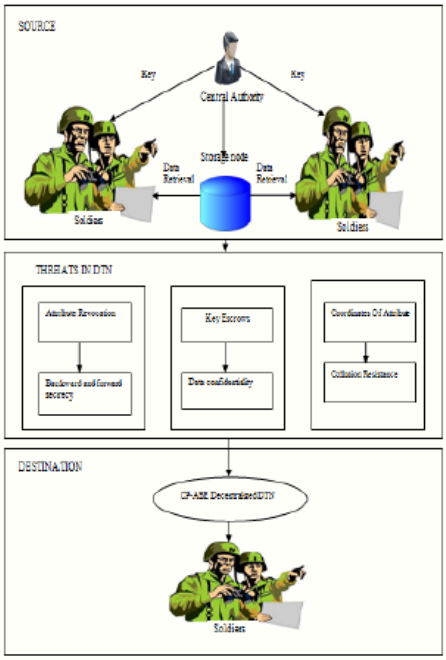

Fig. 2: Architecture of CP-ABE for data retrieval in military networks.

A. System Description and assumptions:

Fig. 2 shows the architecture of the CP-ABE for data retrieval. As shown in Fig. 2, the architecture consists of the following system entities.

1) Key Authorities:

They are defined for key generation and generate public/secret parameters for CP-ABE. The key authorities play a role in two ways central authority and multiple local authorities. It provides the secure and reliable communication path between a central authority and each local authority. In this each local authority controls different attributes and provides attribute keys to users.

2) Storage node:

This is an entity that stores data from senders and provide access to users to work on it. It may be dynamic or static. It is always assumed that storage node to be semi trusted (honest-but-curious).

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 79-85

3) Sender:

This is also an entity that has the secret information or data (e.g., a commander) and it can be stored into the storage node for ease use of sharing the messages or for reliable message delivery to users in the extreme networking environments (e.g., battlefield or hostile regions). Before storing the data into the storage node the sender is responsible for defining the access policy on data by encrypting it.

4) User:

This is a mobile node that uses the data present in the storage node (e.g., a soldier). If a user wants the data to be accessed he must satisfy the access policy of the encrypted data declared by the sender, and is not revoked in any of the attributes, and then he will be able to decrypt the cipher text and obtain the data.

5) Centralized DTN:

In this all or most decision makers (who have the authority, control, and responsibility for the entire organization) are located in one central office (e.g., commander) thus provides access to user in a secure way.

6) Decentralized DTN:

In this all users have their own responsibility to access the data in a secure way. These are applicable only if they are provided with certain access policy and within the region for security purpose.

B. Threat Model:

1) Data confidentiality:

Unauthorized users who do not have enough criteria to satisfy the access policy should be stop from accessing the plaindata in the storage node. Even, unauthorized access from the storage node or key authorities should be prevented

2) Collusion-resistance:

If the users cannot decrypt the ciphertext alone they can be able to use multiple users collude, by combining their attributes. For example, suppose there are users with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually.

3) In ABE, forward secrecy (FS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Backward secrecy is presented. A security-related term, backward secrecy means that a compromise should not compromise any earlier key.

V. *Algorithm Used:*

Zone based routing algorithm:

ZRP [3] exploits the features of both proactive and reactive protocol.The proactive part of the protocol is restricted to a small neighbourhood of a node and the reactive part is used for routing across the network. This reduces latency in route discovery and reduces the number of control messages as well.

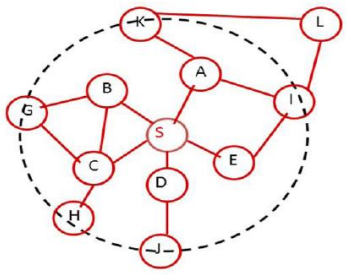

Fig. 3: Architecture of ZRP.

In figure 3: Each node S in the network has a routing zone. This is the proactive zone for S as S collects information about its routing zone in the manner of the DSDV protocol.

In figure 4: The routing in ZRP is divided into two partsis intrazone routing and Interzone routing. First, the packet is sent within the routing zone of the source node to reach the peripheral nodes. Then the packet is sent from the peripheral nodes towards the destination node.

Journal of Industrial Engineering Research, 1(4) July 2015, Pages: 79-85

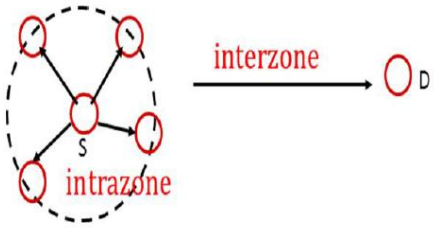

Fig. 4: Intrazone and Interzone routing.

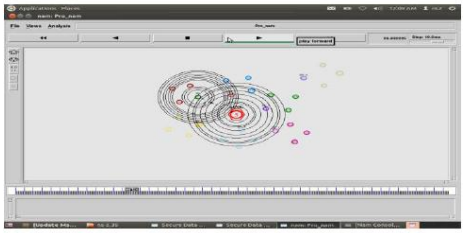

Fig. 5: Transferring Data from Storage Node to Sink Node.

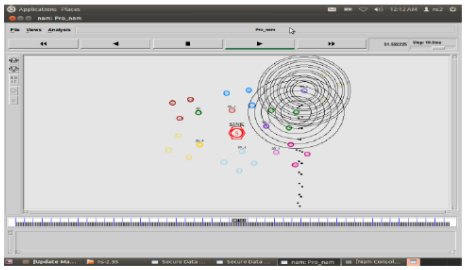

Fig. 6: Packet Loss Due to Uninvited Node.

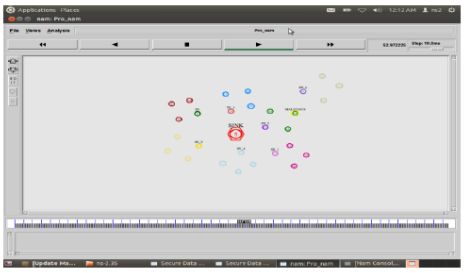

Fig. 7: Finding Malicious Node in a Region.

Fig. 8: Transferring Collected Data to the Sink Nod.

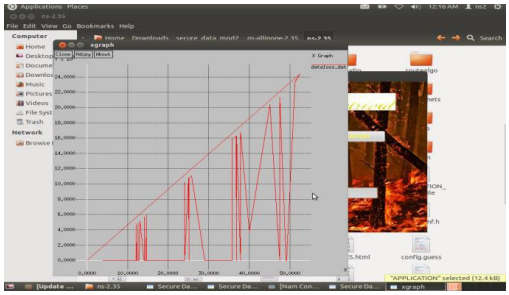

Fig. 9: Graphical Representation.

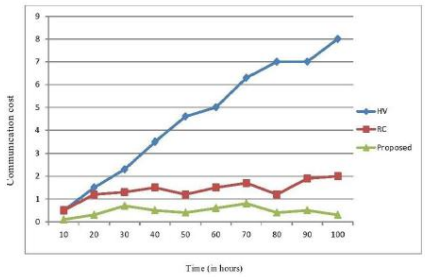

Fig. 10: Performance Evaluation.

Conclusion:

Cp-abe is a scalable cryptographic solution [13] to the access control and secure data retrieval issues [12]. In this paper, 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 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.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang, *2014. "*Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" *in IEEE, ACM*
[2] Xiaohui Liang, Rongxing Lu, Xiaodong Lin and Xuemin (Sherman) Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation" in *IEEE ACM.*
[3] Nicklas Beijar Networking Laboratory, Helsinki University of Technology, "Zone Routing Protocol (ZRP)"
[4] Roy, S. and M. Chuah, 2009. "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep.
[5] Huang, D. and M. Verma, 2009. "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, 7(8): 1526–1535.
[6] Lewko, A. and B. Waters, 2010. "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep, 2010/351.
[7] Goyal, V., O. Pandey, A. Sahai and B. Waters, 2006. "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Security*, 89-98.
[8] Bethencourt, J., A. Sahai and B. Waters, 2007. "Ciphertext-policy attribute based encryption," in *Proc. IEEE Symp. Security Privacy*, 321–334.
[9] Ostrovsky, R., A. Sahai and B. Waters, 2007. "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput. Commun. Security*, 195–203.
[10] Yu, S., C. Wang, K. Ren and W. Lou, 2010. "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 261-270.
[11] Boldyreva, A., V. Goyal and V. Kumar, 2008. "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 417-426.
[12] Pirretti, M., P. Traynor, P. McDaniel and B. Waters, 2006. "Secure attribute based systems," in *Proc. ACMConf. Comput. Commun. Security*, 99-112.
[13] Mittra, S., 1997. "Iolus: A framework for scalable secure multicasting," in *Proc. Acm Sigcomm*, 277 288.
[14] Cheung, L. and C. Newport, 2007. "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Security*, 456-465.
[15] Liang, X., Z. Cao, H. Lin and D. Xing, 2009. "Provably secure and efficient bounded ciphertext policy attribute based encryption," in *Proc. ASIACCS*, 343-352.