ACCESS CONTROL AND SECURE DATA RETRIEVAL BASED ON CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION IN DECENTRALIZED DTNS

Dhiren Kumar Dalai[1], Arunram Ravi[2]
[1, 2] Department of CSE, Anna University, (India)

ABSTRACT

Mobile Nodes in some challenging network scenarios such as disaster recovery areas, military battlefields, hostile region or urban sensing applications suffer from intermittent connectivity and frequent partitions. Disruption Tolerant Network (DTN) Technologies are becoming challenging and successful solution for End To End communication between wireless devices. This allow nodes to communicate with each other in extreme terrestrial networking environments, or planned networks in space .In this Scenario Data to be stored and retrieved from the storage nodes ,since the data is sensitive data one needs to consider the security policies. The attribute-based encryption (ABE) is a promising approach that full fills the requirements for secure data retrieval in DTN .the existing system involves some challenging issues like fine grain access control to contents stored in storage nodes within a DTN. In this paper, we propose an access control scheme which is based on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach which provides a scalable way of encrypting data such that the encrypter defines the attribute set that the decrypted needs to process for decrypting the cipher text. Since the problem of applying CP-ABE in decentralized structure of DTN results inseveral security and privacy challenges with regards to the attribute revocation of all nodes, key escrow and coordination of attributes issued from various authorities. So, data retrieval scheme must be secured for using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently, in addition to that geographical routing is also used for finding the location of the nodes to reduce complexity , communication cost and to increase security. Wealso provide some performance results from our implementation.

Index Terms: Disruption Tolerant Networking (DTN), Node Location, Access Control, Attribute Based Encryption (ABE) Secure Data Retrieval.

I. INTRODUCTION

Now days many computing devices e.g. PDAs, smart-phones, 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. [1] military network environments, connections of wireless devices carried by soldiers may be temporarily disconnected by environmental factors, jamming and mobility, especially when they operate in terrestrial environments. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicatewith each other in these extreme terrestrial environments [2]-[4]. Typically, when there is no end-to-end connection between asource 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.For storage and replicate the data storage node is introduced [5][6]where authorized mobile nodes can access the necessary information quickly. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced [7], [8]. 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. Multiple key authorities manage their attribute independently in DTN [9], [10]. 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 ciphertexts. Especially, ciphertext-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 ciphertext [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 attributes 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 associatedattribute 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.

One more challenging issue is Key escrow problems ,CP-ABE, authority's master secret key is used to generates private keys of users associated set of attributes. So, 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 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. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region 2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

Objectives: 1.Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.

2.Encryptor's can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.

3. The key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture.

4. Location tracking to reduce communication cost.

A. Related Work

ABE comes in two flavors called key-policy ABE (KP-ABE)andciphertext-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. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptorssuch 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], [15] location of node tracked to reduce overhead [18].

II. OVERVIEW OF THE SYSTEM

The proposed system to develop the CP-ABE is a promising cryptographic solution to the access control issues shown in Figure 1.

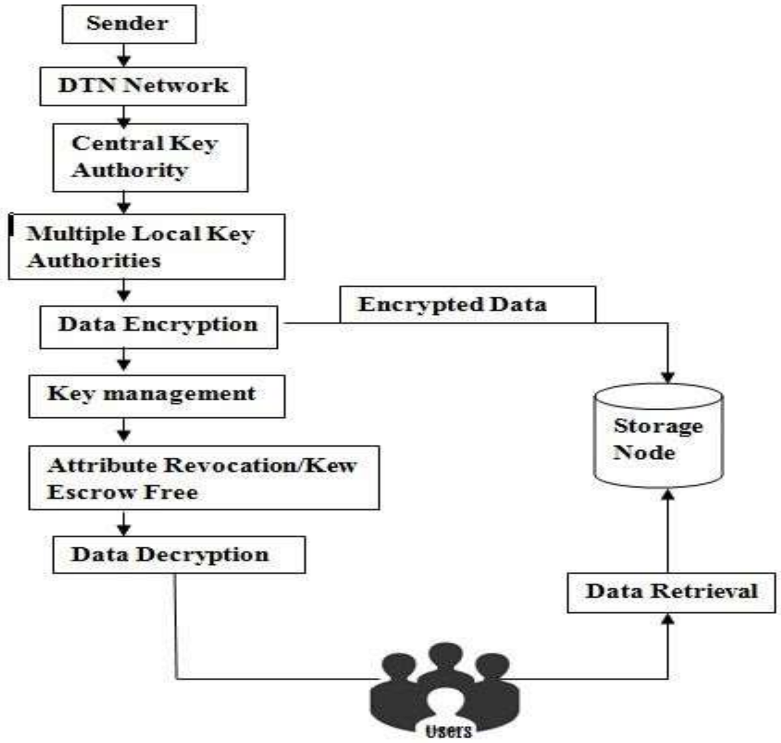


Fig. 1: System Architecture

System Description and Assumptions

Fig. 1 shows the architecture of the DTN. The architecture consists of the following system entities.

1) Key Authorities: They are key generation centres that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority andeach 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 semi trusted, that is honest-but-curious.

3) Sender: This is an entity who owns confidential messagesOr 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 theciphertext and obtain the data.

5) Attribute Revocation: Revocation of users in cryptosystems is a well studied but nontrivial problem. Revocation is even more challenging in attribute-based systems, given that each attribute possibly belongs to multiple different users, whereas in traditional PKI systems public/private key pairs are uniquely associated with a single user. In principle, in an ABE system, attributes, not users or keys, are revoked. Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users. In order to realize this somewhat contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase. The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

6) Location Tracking: A simple scheme is presented for geographic forwarding that is similar to Cartesian routing. Each node determines its own geographic position using a mechanism such as GPS; positions consist of latitude and longitude. A node announces its presence, position, and velocity to its neighbours (other nodes within radio range) by broadcasting periodic HELLO packets. Each node maintains a table of its current neighbours‟ identities and geographic positions. The header of a packet destined for a particular node contains the destination's identity as well as its geographic position. When node needs to forward a packet toward location P, the node consults its neighbour table and chooses the neighbour closest to P. It then forwards the packet to that neighbour, which itself applies the same forwarding algorithm. The packet stops when it reaches the destination.

III. PROPOSED SCHEME

In this section, we provide a multiauthority 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

Scheme Construction

The concept of CP-ABE is

- Private key assigned to “attributes”
- Cipher text associated with “access policy”
- Can decrypt only when attributes satisfy policy.

Central key Authority:

1. Choose a random exponent β∈ R Z*p.

Let h=g β

2. Masters (secret key)/public key

PKCA=h MKCA=β.

Local Key Authority

1. Choose a random exponent αi∈ R Z*p.

2. Masters (secret key)/public key pair is

PKAi=e (g,g)αi,MK Ai=αi.

An efficient and secure data retrieval method using CP-ABE is used 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 local and central might be compromised or not fully trusted.

Key Generation: (MK, L): The key generation algorithm runs by CA. It takes as input the Master key of CA and the set of attributes L for user, then generate the secret key SK

3.1 Algorithm for Key Generation

A trusted party chooses and publishes a (large) prime *p* and an integer *g*having large prime order in F*p

1. Select a large prime number p.

i. Choose a secret integer a.

ii. Compute A ≡ ga(mod p).

iii. Choose a secret integer b.

iv. Compute B ≡ gb(mod p).

2. Masters (secret key)

Compute the number Ba(mod p). Compute the number Ab(mod p).

The shared secret value is Ba ≡ (gb)a ≡ gab ≡ (ga)b ≡ Ab(mod p).

Data Encryption: Here when a sender wants to deliver its confidential data M, he defines the tree access structure T over the universe of attributes L, encrypts the data under to enforce attribute-based access control on the data, and stores it into the storage node. The encryption algorithm takes as input the message M, public parameter PK and access structure A over the universe of attributes. Generate the output CT such that only those users who had valid set of attributes that satisfy the access policy can only able to decrypt. Assume that the CT implicitly contains access structure A.

Data Decryption: When a user receives the ciphertext from the storage node, the user decrypts the ciphertext with its secret key. The decrypt algorithm run by user takes input the public parameter, the ciphertext CT contains access structure A and the secret key SK contain of user attribute set S. If S satisfies the access tree then algorithm decrypt the CT and give M otherwise gives "ϕ".

Key Update (MK, SK, old value, new value): The key updating algorithm runs by CA. It takes as input the master key of CA, old SK and old attribute value old value, and then updates the secret key SK by updating (add/delete/update) old value with new value.

3.2 CP-ABE for Data Retrieval

We provide a 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. Data confidentiality on the stored the data against unauthorized users can be trivially guaranteed .Which shown in Fig.2

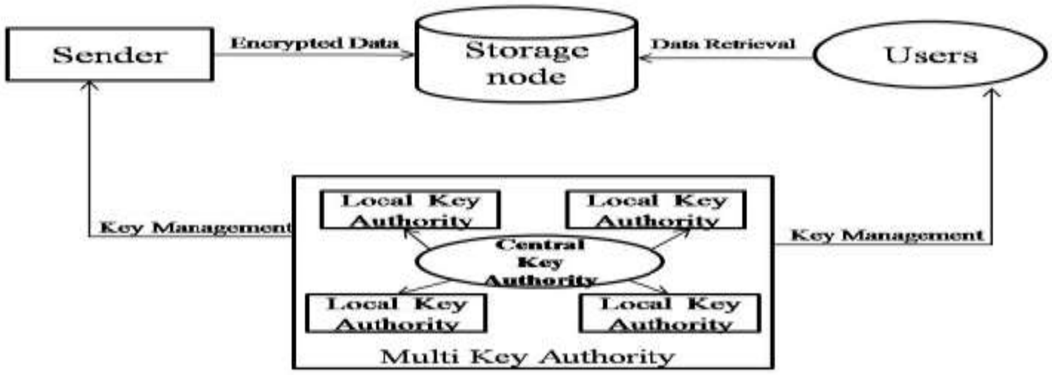


Fig. 2: Data Retrieval

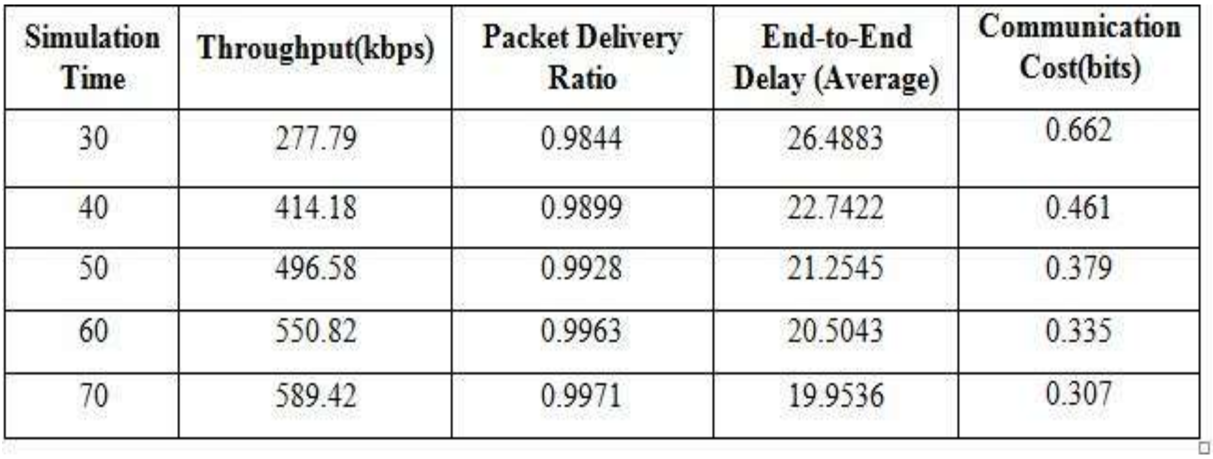
3.3 Location Tracking

Apart from this location of nodes also detected and intimates the position to neighbour nodes. Each node determines its own geographic position using a mechanism such as GPS; positions consist of latitude and longitude. A node announces its presence, position, and velocity to its neighbours by broadcasting periodic HELLO packets. Each node maintains a table of its current neighbour's identities and geographic positions. The header of a packet destined for a particular node contains the destination's identity as well as its geographic position. When node needs to forward a packet toward location, the node consults its neighbour table and chooses the neighbour closest to it. It then forwards the packet to that neighbour, which itself applies the same forwarding algorithm. The packet stops when it reaches the destination.

IV. RESULTS

The proposed system Access control and Secure data retrieval based on CP-ABE implemented in NS2Simulator. Here we perform access control and secure data retrieval by CP-ABE as well as location of node also tracked by using geographical routing protocols .which helps to identify the position on nodes and to control the access of data .Table 1shows all evaluation factors calculated values like communication cost end to end delay, throughput and packet delivery ratio .and in Fig. 4 shows the plotted graph of them.

Table 1(Evaluation Values)



Simulation Time	Throughput(kbps)	Packet Delivery Ratio	End-to-End Delay (Average)	Communication Cost(bits)
30	277.79	0.9844	26.4883	0.662
40	414.18	0.9899	22.7422	0.461
50	496.58	0.9928	21.2545	0.379
60	550.82	0.9963	20.5043	0.335
70	589.42	0.9971	19.9536	0.307

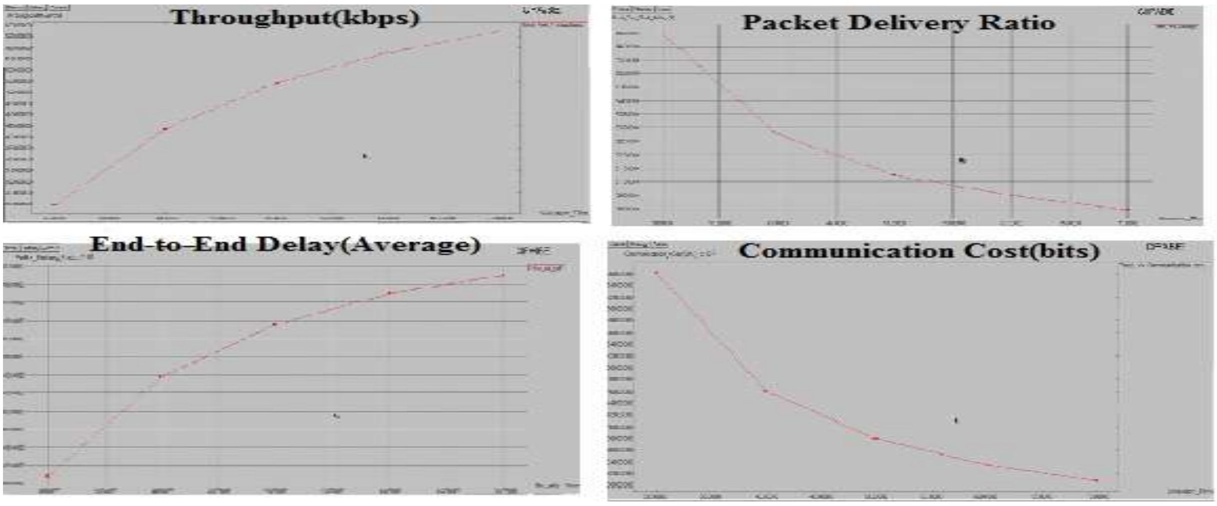


Fig. 4:Performance Graph

V. CONCLUSION

Disruption Tolerant Network (DTN) Technologies are becoming challenging and successful solution for End To End communication between wireless devices. Now DTN are becomes successful solution in hostile area like military applications that allows wireless devices .Confidential data can be access by using external storage nodes .CP-ABE is a successful cryptographic solution to access control and secure data retrieval in decentralized DTN networks 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. In the proposed system location of node also identified using geographical routing protocol, which improve performance and reduce communication cost.

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] JunbeomHur and Dong Kun Noh, "Attribute-Based Access Control with EfficientRevocation in Data Outsourcing Systems" IEEE Transactions On Parallel And Distributed Systems, Vol. 22, NO. 7, JULY 2011,pp.1214-1221

[4] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM,2007, pp. 1–7.

[5] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute- based encryption," in Proc. ACM Conf. Comput. Common Security, 2009, pp. 121–130.

[6] Improving Security and Efficiency in Attribute-Based Data Sharing JunbeomHur IEEE Transactions on Knowledge And Data Engineering, VOL. 25, NO. 10, OCTOBER 2013.pp.2271-2282

[7] M. M. B. Tariq, M. Ammar, and E. Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACMMobiHoc, 2006, pp. 37–48.

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. ACM Conf. Comput.Commun. Security, 2009, pp. 121–130.

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

[15] 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.

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

[17] M.Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks", in Proc. IEEE MILCOM, pp.1–11, 2006.

[18] Rong Ding and Lei Yang," A Reactive Geographic Routing Protocol for Wireless Sensor Networks", in Computer Science Department, Beihang University, Beijing, pp.1-11, 2006

BIOGRAPHY

[1]**Dhiren Kumar Dalai** received his B.E (CSE) degree from Anna University, India in 2010. He is pursuing M.E. in Computer Science, College of Engineering, Guindy, Anna University,Chennai. His research interests are in the area of Network Security.

[2]**Arunram Ravi** received his B.E (ECE), from Anna University in Nov 2013. He is pursuing M.E. in Computer Science, College of Engineering, Guindy, Anna University,Chennai. Analog and digital communication systems, computer networks.