ISSN No: - 2456 – 2165

Trust Based CP-ABE for DTN

[1]Dhiren Kumar Dalai
Department of CSE
Assistant professor, MRIT
dhirenbiren@gmail.com

[2]N.Venkatesh
Department of CSE
Assistant professor, MRIT
narojuvenkat@gmail.com

***Abstract*—In extreme wireless network environment Mobile Nodes suffers from inter communication such as military networks, hostile environments. Disruption Tolerant Network (DTN) technologies gives challenging and successful solution for end to end connection between nodes. In this network the encrypted data is stored in the external storage node and retrieved it by decryption from it, as the confidential data to be retrieve securely it needs to be consider some security schemes. Attribute-Based Encryption (ABE) is a promising approach to cryptography that full fills the requirements for secure data retrieval in DTN. The existing system involves some challenging issues like intimacy, attribute update and trust management and in Ciphertext Policy Attribute-Based Encryption (CP-ABE) having key updating issue. To overcome this we proposed a scheme for data accessed which is based on the Trust based Ciphertext Policy-Attribute Based Encryption (TCP-ABE) scheme which provides a scalable way for confidential data retrieval and reduce complexity. In addition the location of node also traced by using GPS protocols to make more flexible and easy communication between surrounding nodes. Here various key authorities maintain their attributes individually; in addition to that trust value calculated for each node and updated it in trust table each and every time. This proposed method provides trust based encryption technique when compared with the existing approach.**

Index Terms: *Disruption Tolerant Networking (DTN), Node Location, Access Control, Attribute,trust based chypertext - Attribute-Based Encryption(TCP-ABE) Based Encryption (ABE) Secure Data Retrieval, Encryption, Security.*

I. INTRODUCTION

Data confidential and secure data retrieval policy plays main role in data communication as well as crypto system. The concept of attribute-based encryption (ABE) is a promising approach that provides the requirements for secure data retrieval in DTNs [7]. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts.

The ciphertext 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. Implementation of CP-ABE for decentralized DTNs [16] where multiple key authorities manage their attributes independently. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture proposed a decentralized approach [8].

Attribute-based encryption (ABE) full fills the requirements for secure data retrieval in DTNs. It provides an access control over encrypted data using access policies and attributes among private keys and cipher texts [5]. Especially ciphertext-policy 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. 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 [2]. But in CP-ABE is used to generate a private key of user based on their attribute keys [6]. Every time when a user enters or removes from certain group then immediate key revocation is done. Updating attribute is not so efficient for every change and it produces high computation complexity and communication cost as revocation [9] of any attribute or any single user in an attribute group would affect the other users in the group. So here proposed trust based CP-ABE with tracking the location of nodes [1].

II. SYSTEM ARCHITECTURE

- The proposed system to develop the Trust based CP-ABE in decentralized DTNs for secure data retrieval.
- Created a simulation environment on wireless network topology and implemented with existing protocol and with more number of nodes. Source node will send the data to destination node through intermediate nodes in the networks. Here the packets transfer using general network, so that we can show how the data transmission occurs in general wireless networks. 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. Secure data retrieval scheme using trust based CP-ABE for decentralized DTNs where the multiple key authorities manage their attributes independently. Immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability.

ISSN No: - 2456 – 2165

In Trust based 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 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. Key escrow problem is resolved by an escrow-free key issuing protocol that exploits it. The characteristic of the decentralized DTN architecture proposed a decentralized approach. There are key generation centres that generate public parameters for CP-ABE. It may consist of one central authority and multiple local authorities. For secure communication key authority generate attribute keys to the user. The next step is to encrypt the data to be stored in storage node securely.On receiving the request query from user the storage node respond to the user. Here sender can define the access policy under attributes. When user receives the cipher text from storage node, the user decrypts the ciphertext with its secret key. 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.

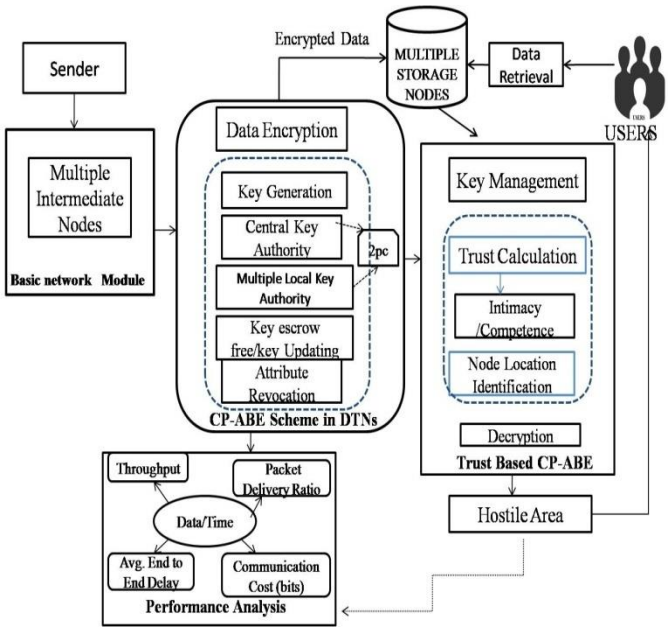


Fig.1. System Architecture

On receiving the request query from user the storage node respond to the user. Here sender can define the access policy under attributes. When user receives the cipher text from storage node, the user decrypts the ciphertext with its secret key. 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 [11] 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.An efficient and secure data retrieval method using trust based CP-ABE is used for decentralized DTNs where multiple key authorities [3] 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. Trust value for each neighbour node is calculated, according to high trust value data can be pass apart from this node location also traced to reduce the selfishness [12]. First this project will analyze and compare the efficiency of the proposed scheme to the multi authority and trust values for trust based CP-ABE Schemes in theoretical aspects [4] make a compression with existing system. Then we will demonstrate in the network simulation in terms of the communication cost.

III. MODULE DESIGN

1. CP-ABE scheme
   - Encryption & Decryption
   - Attribute Revocation
2. Trust based CP-ABE Scheme
   - Trust Evaluation
   - Node Location Identification
3. Data Retrieval

3.3.1 CP-ABE SCHEME

The concept of CP-ABE is Private key assigned to “attributes” Cipher text associated with “access policy”Can decrypt only when attributes satisfy policy.

IV. KEY AUTHORITY

They are key generation centers that generate public/secret parameters for Trust based CP-ABE. The key authorities consist of a central authority and multiple local authorities. Generate keys as private and masters keys by key Authorities as Central Authority and having many Local Authority for which multiple key authorities manage their attributes independently. The key update procedure is launched by sending a join or leave request for some attribute group from a user who wants to hold or drop the attribute to the corresponding authority. On receipt of the membership change request for some attribute Groups; it notifies the storage node of the event without loss of generality.

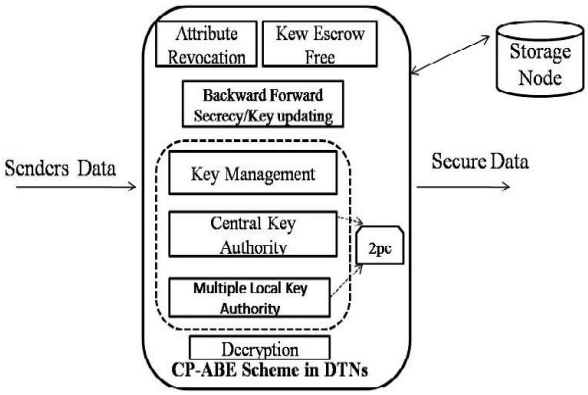


Fig 2. CP-ABE Scheme in DTNS

ISSN No: - 2456 – 2165

Local Key Authority:

Choose a random exponent αi∈ R Z*p.

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 by equation

V. 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

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).

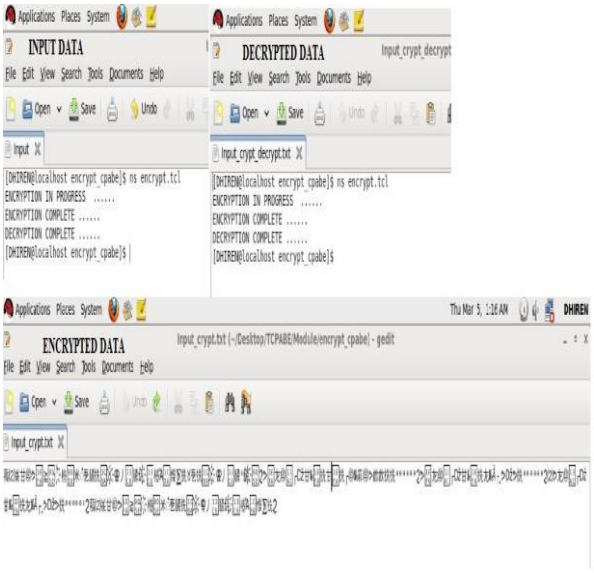
VI. DATA ENCRYPTION AND DECRYPTION

Data Encryption: Here when a sender wants to deliver its confidential data , he defines the tree access structure over the universe of attributes , 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 [13], public parameter PK and access structure A over the universe of attributes. Generate the output CT such that only those users.

VII. ATTRIBUTE REVOCATION

In general, this revocation technique would require each message to be encrypted with a modified access tree T0, which is constructed by augmenting the original access tree T with an additional list of revoked user IDs. Formally, the new access structure T0 is as follows: who had valid set of attributes that satisfy the access policy can only able to decrypt. Assume that the CT implicitly contains access structure.

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".



T0 = (T AND ((NOT User X1) AND (NOT User X2) . . . AND (NOT User Xm))

Where users X1, X2. Xm have been revoked.

VIII. 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, this applied by equation 3.4.

A. Algorithm for Attribute Revocation

- Backward secrecy

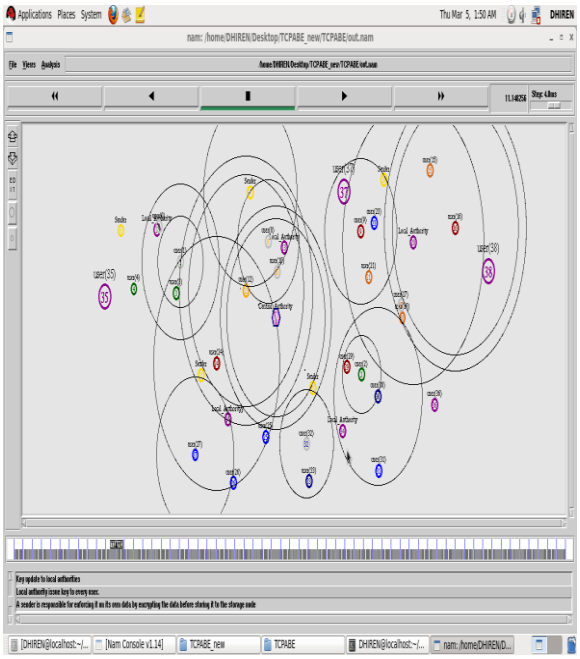
1. User that satisfies the access policy holds the attribute to prevent from plain text
   a) All the attribute encrypt with secret key
   b) Re encrypted by the storage node
   c) Attribute also re encrypted with updated attribute group keys.
2. If the user has stored the previous cipher key exchanged

ISSN No: - 2456 – 2165

a) Holding attributes satisfy the access policy
b) Backward secrecy of the data is guaranteed.

- *Forward Secrecy*

1. Drops attribute should be prevent from accessing the plain text
a) Attribute group keys are also updated and delivered to the valid members.
b) Encrypted with secret key
c) Cipher text re encrypted using storage node with random.
2. After revocation due to blindness results from newly updated group
a) Revoked from the attribute group and stored it.
b) Forward secrecy of the stored data is guaranteed.



IX. TRUST BASED CP-ABE SCHEME

In trust based CP-ABE the same CP-ABE is implemented apart from this the trust value is calculated among the all nodes for communication and node location also traced by using GPS protocols.

A. Trust Evaluation

The trust management is achieved by first determining the best trust formation model given a set of model parameters specifying the environment conditions, and then at runtime this trust system learns and adapts to changing environment conditions by using the best trust formation model identified from static analysis.
Algorithm for calculation trust value

$$A = \sum_{i=1}^{n} T_y(i) \qquad 3.5$$

Where:
Ty (i) – Trust value of the ith trust category .
n- number of trust categories .

$$B = \frac{\sum_{i=1}^{n} T_j(X)}{n}$$

Where:
Tj (X)- Trust value of node J on X.
n- number of surrounding nodes.

C= F1 (A, B)

$$D = \sum_{i=1}^{n} T_k(X)$$

Where:
Tk (X)- The risk value of kth trust on X.
n- number of trust categories .
E = F2(C,D) = F2(F1(A,B),D)

Ty(x) = A, if the trust from previous interactions is enough B, if the trust from recommendations is enough
C. if j(A.B) value is enough
D, if the D is positional trust is enough
E, if j(C,D) value is enough

Value	Label	Description
+1	Blind trust	Based on previous experience.
> .75	Very high	Based on trust experience and recommendation
.5 to .75	High trust	Based on recommendation.
.25 to .5	Medium	Based on trust recommendation and risk.
0 to .25	Low trust	Dispositional trust (risk)

Table . Possible Trust Values

According to the above trust evaluation algorithm the trust value is evaluated .each and every node trust value calculated and noted in trust table no 3.1 various possible trust values are comes and it represented in a table 3.1 .all possible trust values categorised as blind ,high medium and low trust values and calculated values comes from the equation 3.5.

ISSN No: - 2456 – 2165

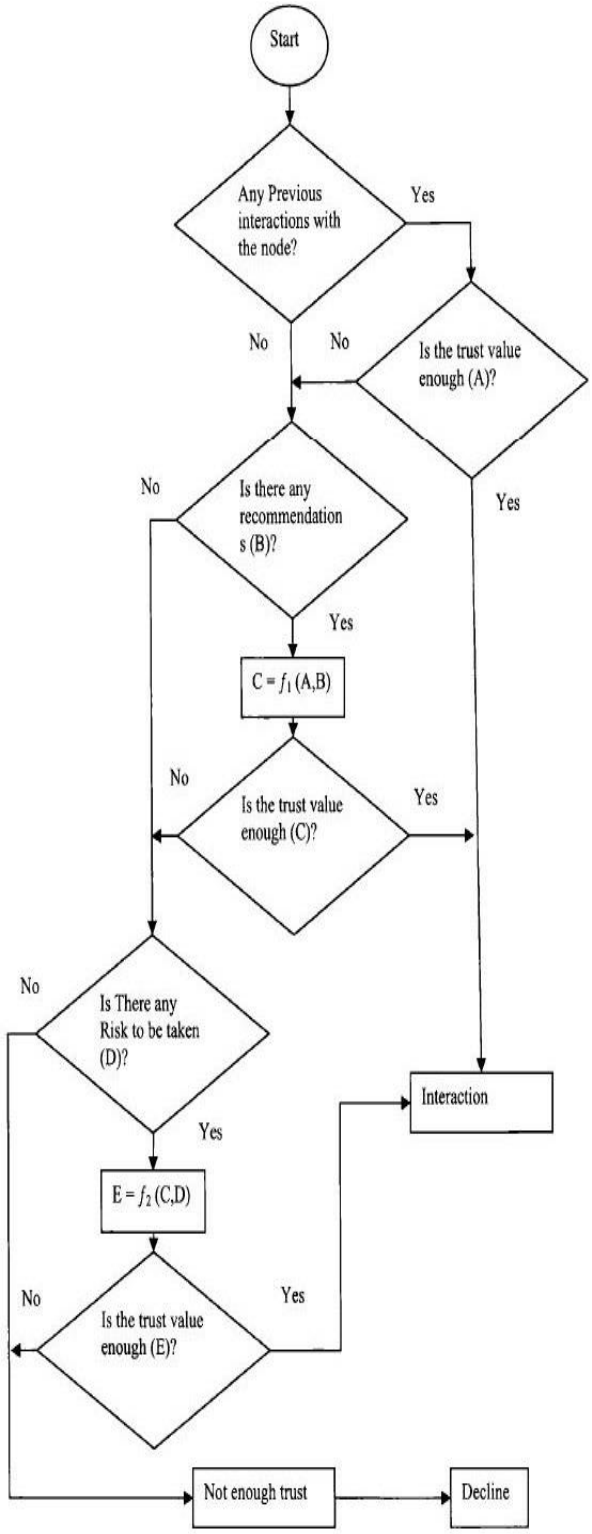


Fig 3. Trust Evaluation

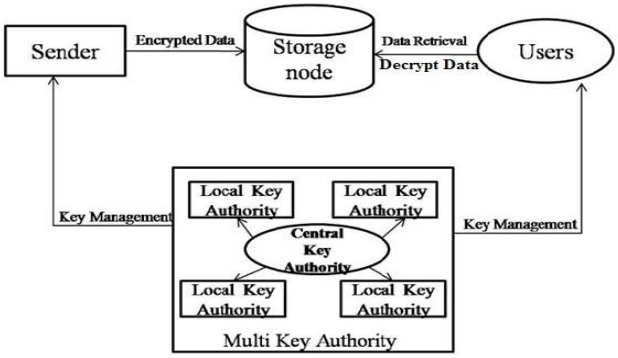
X. NODE LOCATION IDENTIFICATION

The geographical routing is also known as position-based routing or geometric routing is a technique to deliver a message to a node in a network over multiple hops by means of position information. Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location [14]. By using this routing algorithm the location information can be obtained

A. Data Retrieval

The secure data can be retrieval when the user comes to the network by using its secret key. The users retrieve the data from the storage node and decrypt the data if the key mismatch the key authority drops the node. The storage node [16] keeps the encrypted data of the sender. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced. The user get the ciphertext data from the storage node and decrypt the with its secret key .if it miss match with the master key and trust value it will detect and consider as a malicious node and drop the node.

.



B. Data Retrieval

In the above fig 3.4 shows how multiple storage nodes manipulate store and forward scenario. Here the multiple storage nodes receive the encrypted data stored and which retrieved by decryption with its secret key which created by key Authority.

Simulation Time(Sec)	Throughput (Kbps)	Packet Delivery Ratio	End-to-End Delay (Average in Sec)	Communication Cost(Bits)	Intimacy(bits)
30	277.79	0.9891	5.911	0.094	0.9092
40	414.18	0.9898	5.751	0.066	0.9191
50	496.58	0.9938	5.674	0.050	0.9213
60	550.82	0.9945	5.628	0.041	0.9287
70	589.42	0.9955	5.597	0.034	0.9345

Table . Performance of Trust based CP-ABE

Below fig. shows the graphical representation for the performance measures shown in the Table 4.1.How performance will increase by using Trust based CP-ABE in the Decentralized DTNs is our proposed system. There is a comparison with existing system and the trust evolution graph.

ISSN No: - 2456 – 2165

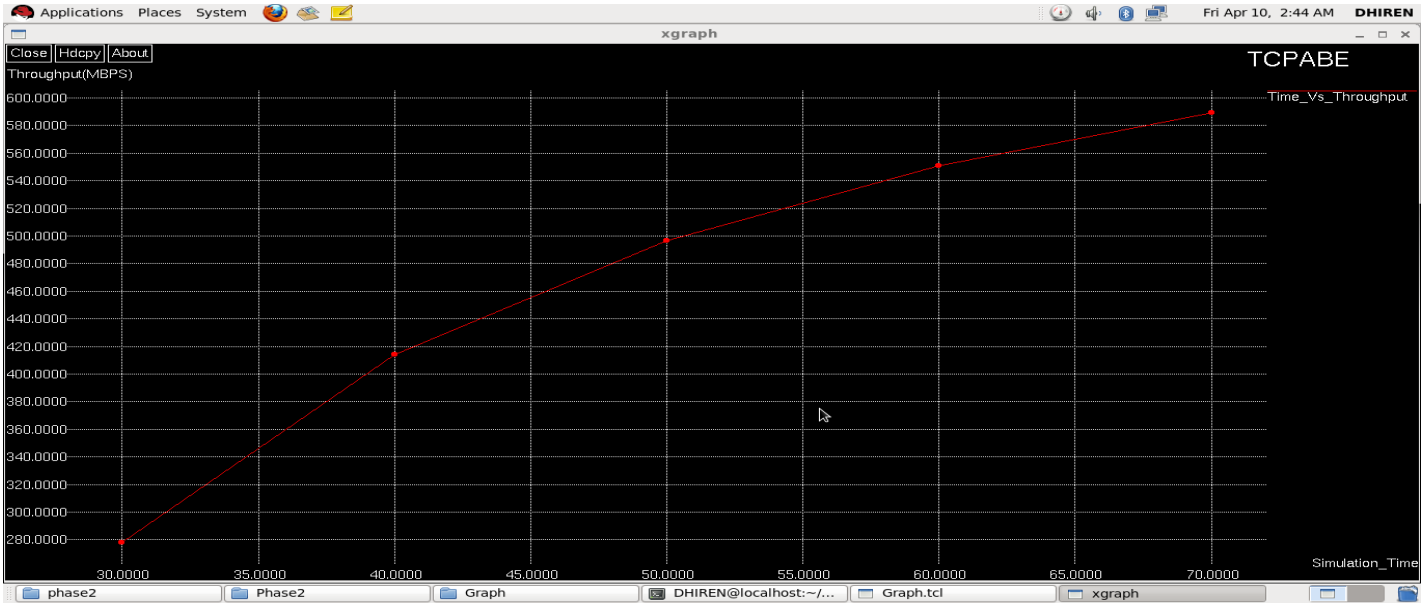


Fig. Throughput

XI. NODE LOCATION

The geographical routing is also known as position-based routing or geometric routing is a technique to deliver a message to a node in a network over multiple hops by means of position information. Routing decisions are not based on network addresses and routing tables; instead, messages are routed towards a destination location [14]. By using this routing algorithm the location information can be obtained. This is shown in fig.4.6.here used distance formula to calculate distance between the two neighbour nodes.

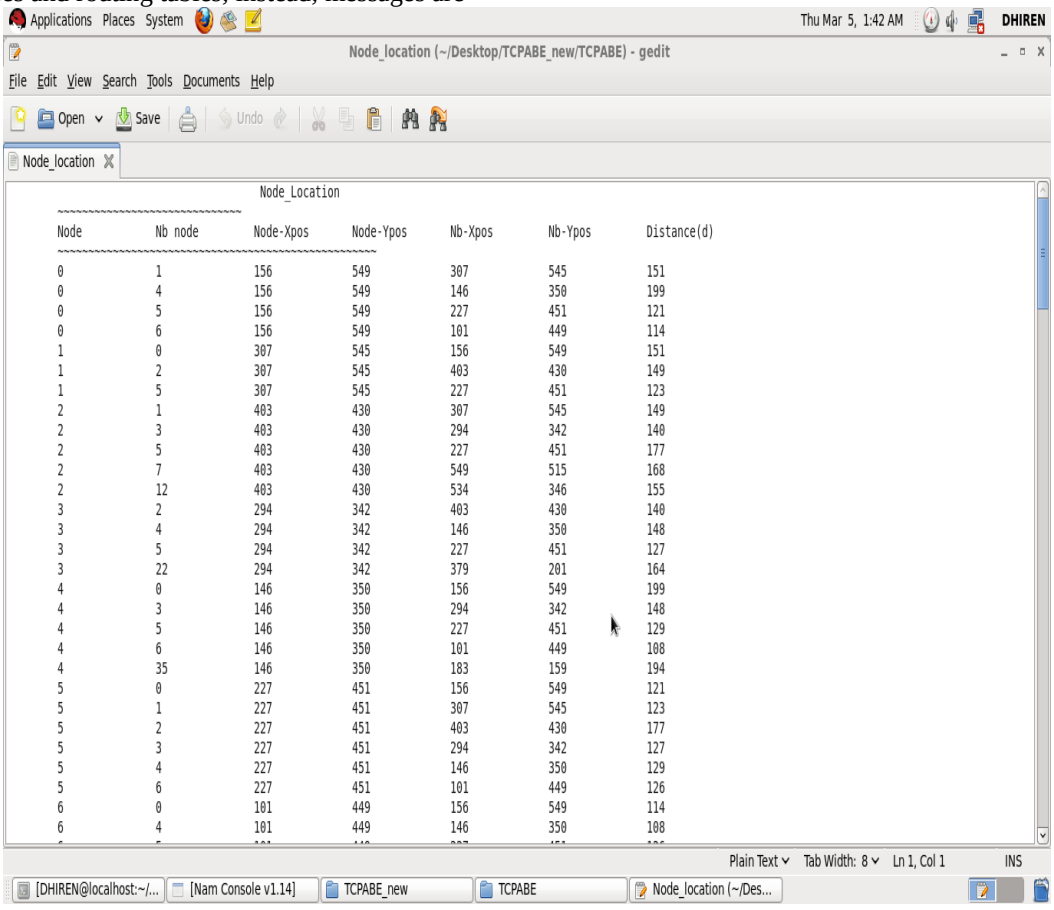


Fig 4.6.. Node Location

This Fig.4.6 shows the location of each node and distance between each node from source to destination. Apart from this the hop also counted and shown through which it passes through.

ISSN No: - 2456 – 2165

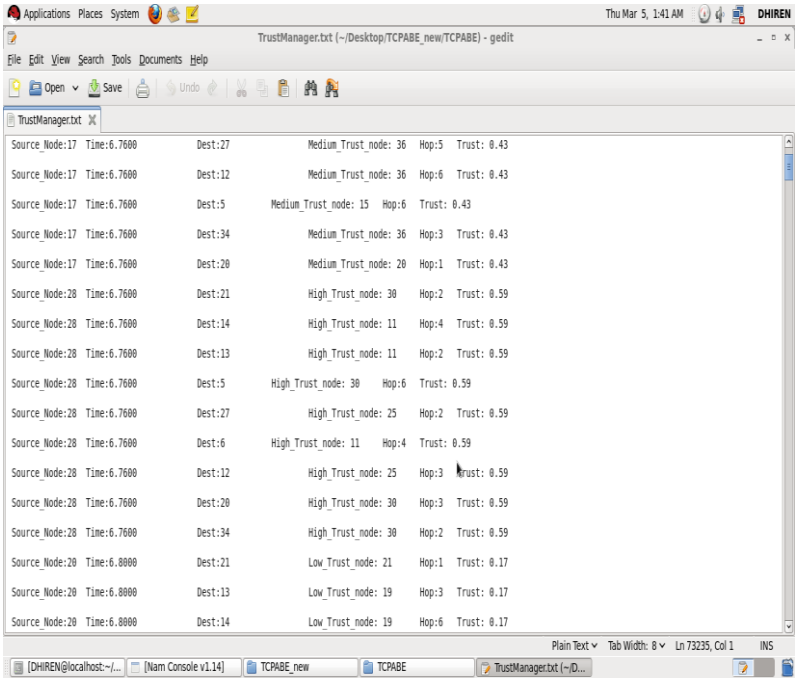


Fig 4.7.. Possible Trust Values

The trust values of every node at each time noticed in the trust table Fig.4.7 and the change of trust values shown in Fig.4.8

Fig 4.8.Trust Variation

A. Performance Comparison

In this section Table 4.2 compares the proposed system evolution parameters with the popular CP-ABE. Here taken different simulation time and reported the evolution parameter and make a comparison with the existing system. Comparison of evaluation parameters is shown in Table 4.2 and corresponding graph is shown in Fig.4.9.

ISSN No: - 2456 – 2165

Table 4.2 Packet Delivery Ratio Comparison

Time(sec)	CP-ABE	TCP-ABE
30	0.9849	0.9891
40	0.9859	0.9898
50	0.9892	0.9939
60	0.9934	0.9945
70	0.9945	0.9949

In Table the packets delivery Ratio for the existing system and there is a comparison to proposed system. It shows that the delay of proposed system is more as compare to existing system, this shown in Fig.4.9.

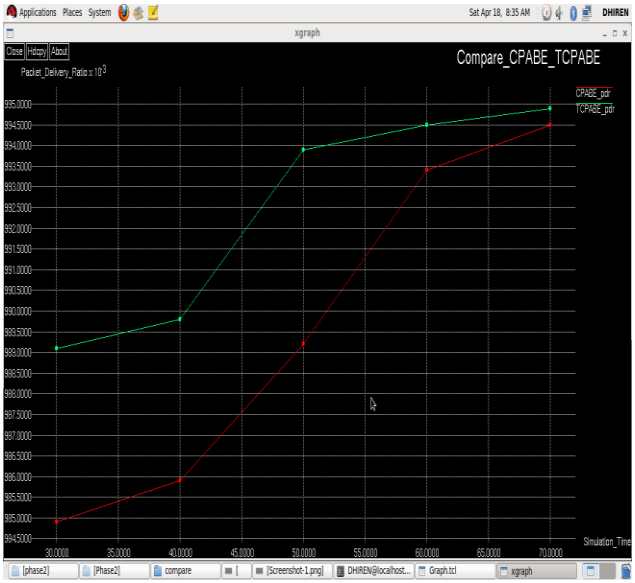


Fig 4.9. PDR Comparison Graph

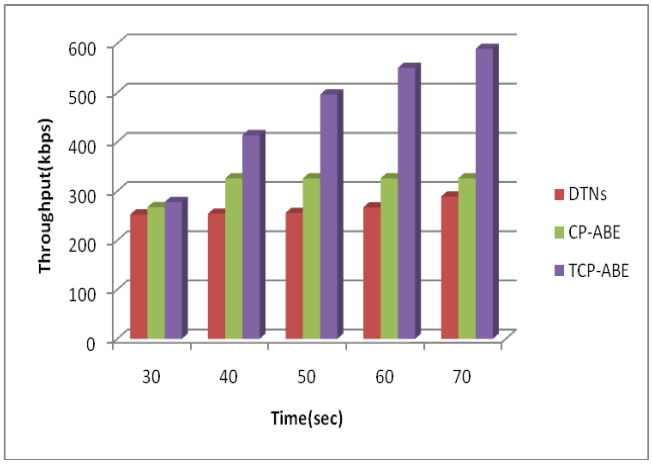


Fig 4.10. Throughput

XII. 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. TCP-ABE is a successful cryptographic solution to access control and secure data retrieval in decentralized DTN networks. Here multiple key authorities manage their attributes independently. Trust value evaluated among all nodes and updated each and every time in trust table. Apart from this location of nodes also traced by using GPS protocols. For which improve performance and reduce communication cost.

REFERENCES

[1]. S.Revathi and Raghavendra, "Advanced Data Access Scheme in Disruption Tolerant Network", International Journal of Innovative Research in Computer and Communication Engineering, pp. 1-7, October 2014.

[2]. Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 10, pp. 2271-2282, October 2013.

[3]. Rama Sundari Battula and O. S. Khanna, "Geographic Routing Protocols for Wireless Sensor Networks: A Review ", International Journal of Engineering and Innovative Technology, Volume 2, Issue 12, pp.39-42, June 2013.

[4]. Junbeom Hur and Dong Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 7, pp. 1214-1221, July 2011.

[5]. John Brent and Amit Sahai "Ciphertext-Policy Attribute-Based Encryption", International Association for cryptographic Research, In Proceedings of IEEE SP, Oakland pp 53-70, 2011.

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

[7]. S. Roy and M. Chuah, "Secure Data Retrieval Based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) System for the DTNs", Lehigh CSE Tech. Rep., pp.1-11, July 2009.

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

[9]. Dhiren Kumar Dalai, P. Elumalaivasan, Sreejith V. P., "An Analysis on Attribute based Encryption for Secure Data Retrieval in DTNs", International Journal of Advance Research in Science and Engineering, Volume No. 04, Issue No. 02, February 2015, pp. 169-175.

ISSN No: - 2456 – 2165

BIOGRAPHY

[1] **Dhiren Kumar Dalai** received his M.Tech (CSE) degree from Anna University, India in 2015. Presently he is working as Assistant professor in the Computer Science and Engineering Dept, in MRIT (JNTU) Hyderabad. His research interest is in the area of Network Security.

[2]**N.venkatesh** working as Assistant professor in the Computer Science and Engineering Dept, in MRIT(JNTU)Hyderabad.