CCP-ABE Technique for Decentralized Disruption Tolerant Military Networks

Ch. Gopala Krishna [1], M. Apparao [2]
[1]M. Tech, [2] Senior Assistant Professor
[1]Department of Information Technology, [2]Department of Information Technology
[1]AITAM, Tekkali, A.P., India, [2]AITAM, Tekkali, A.P., India

***Abstract* - Mobile nodes in military environment such as a battle field or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-Tolerant Network (DTN) innovations are getting to be effective arrangements that permit remote gadgets conveyed by fighters to impart with one another and access the confidential data or order dependably by abusing outer stockpiling hubs. A portion of the most difficult issues in this situation are the requirement of approval approaches and the strategies upgrade for secure information recovery. In the existing system for secure transactions Attribute-Based Encryption (ABE) is used. In the proposed system Constant Cipher text Policy- Attribute Based Encryption (CCP-ABE) is a promising cryptographic technique for the entrance control issues in military networks. Constant Cipher text-Policy ABE (CCP-ABE) provides ascalable way of encrypting data such that the encrypted defines the attribute set that the descriptor 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.**

The issue of applying CCP-ABE in decentralized DTN presents a few securities and protection challenges with respect to the quality renouncement, key escrow, and coordination of characteristics issued from diverse powers. In this paper, we propose a safe information recovery plan utilizing CCP-ABE for decentralized DTNs where different key powers deal with their qualities autonomously. We exhibit how to apply the proposed component to safely and proficiently deal with the confidential information disseminated in the interruption tolerant military system.

***Keywords* - Access control, characteristic based encryption (ABE), Disruption-tolerant network (DTN), multiauthority, secure information recover**

1. INTRODUCTION

In numerous military system situations, associations of remote gadgets conveyed by troopers may be incidentally detached by sticking, natural elements, and versatility, particularly when they work in threatening situations. Disruption-tolerant network (DTN) innovations are getting to be fruitful arrangements that permit hubs to correspond with one another in these compelling systems administration situations. Normally, when there is no limit to-end association between a source and a destination match, the messages from the source hub may need to sit tight in the middle of the road hubs for a generous measure of time until the association would be in the end built up.

The idea of trait based encryption (ABE) is a promising approach that satisfies the necessities for secure information recovery in DTNs. ABE highlights an instrument that empowers an entrance control over scrambled information utilizing access strategies and credited properties among private keys and figure writings. Particularly, Constant Ciphertext-arrangement ABE (CCP-ABE) gives a versatile method for encoding information such that the encryptor characterizes the characteristic set that the decryptor needs to have keeping in mind the end goal to decode the ciphertext. Hence, distinctive clients are permitted to unscramble diverse bits of information per the security arrangement. In any case, the issue of applying the ABE to DTNs presents a few security and protection challenges. Since a few clients may change their related qualities sooner or later (for instance, moving their area), or some private keys may be traded off, key disavowal (or upgrade) for every characteristic is important to make frameworks secure.

Constant Cipher text Policy Attribute-Based Encryption (CCP-ABE)[1], is a very active and live domain in recent years as far as security is concerned. In constructing CCP-ABE, an attribute is a descriptive string associated with an entity and each entity may be tagged with multiple attributes. Many entities may share common attributes, which allow message encryptors to specify a secure data access policy by composing multiple attributes through logical operators such as \AND", \OR", etc. For decrypting the message, the decryptor's attributes need to satisfy the access policy. These unique features of CCP-ABE solutions make them appealing in many systems that require the expressive data access control for a large numbers of users. But with this unique feature, there is a major problem of the existing CCP-ABE schemes, linearly increasing cipher text. In the CCP-ABE,the size of a cipher text increases linearly with respect to the number of included attributes. For example, the message size CCP-ABE may start at about 650 bytes, and each additional attribute adds about 300 bytes.

In the event that the key power is traded off by foes when conveyed in the unfriendly situations, this could be a potential danger to the information classifiedness or protection particularly when the information is exceptionally delicate. The key escrow is an inborn issue even in the various power frameworks the length of every key power has the entire benefit to produce their own quality keys with their own particular expert privileged insights. Since such a key era instrument taking into account the single expert mystery is the essential strategy for the greater part of the hilter kilter encryption frameworks, for example, the

characteristic based or personality based encryption conventions, uprooting escrow in single or various power CCP-ABE is a crucial open issue.

Figure 1 Architecture of secure data retrieval in a disruption – tolerant military network.

2. LITERATURE SURVEY

J. Burgess et al [2], proposed in their work In CCP-ABE, is taken for the encryption arrangement and in the exchanged information is made to this stride however a key is just made regarding a qualities set. CPABE is more suitable to DTNs than KP-ABE in light of the fact that it empowers encryptions, for example, an authority to pick an entrance strategy on credits and to scramble classified information under the access structure by means of scrambling with the comparing open keys or traits ABE comes in two flavors called key-approach ABE (KP-ABE) and figure content arrangement ABE (CPABE).In KP-ABE, the encoded just gets the chance to mark a figure content with an arrangement of properties. The every client is having the diverse strategy from the key power that decides which figure writings he can unscramble and issues the way to each client by inserting the arrangement into the client's key.

S.Sarany, B.Suganya Devi [3], proposed in their work Disruption tolerant networking (DTN) technology is designed to deal with the intermittent connectivity among mobile nodes due to mobility, short range radios or terrain obstacles. Our schemes utilize both query and data replications to enhance the query success rate. Besides designing efficient query and data dissemination schemes, one needs to consider the security aspects since sensitive data should only be accessed by authorized personnel. In this paper, we present a data-centric security solution for an information retrieval system which we design for DTN environments through the Access Control mechanism through Multi Authority specific Attribute based encryption (MA-ABE). We also describe the preliminary prototype that we have built. Both theoretical analysis and simulation results demonstrate that our proposed scheme is more efficient than the CP-ABE scheme in terms of computational and communication overhead under comparable security levels while providing message and Identity privacy.

VangaOdelu et al [4], proposed in their work a novel ECC-based CP-ABE-CSSK scheme with the constant size secret keys with an expressive AND gate access structure without using bilinear maps. To the best of our knowledge, it is the first ECC-based CP-ABE scheme. In addition, the proposed CP-ABE-CSSK offers the constant size secret keys, which is as small as 320-bits for the 80-bit security. The CP-ABE-CSSK also significantly reduces the encryption and decryption costs as compared to the related existing schemes in the literature. We have showed that our scheme is secure against possible known attacks, such as key recovery and collision attacks. In addition, we have shown that our scheme is secure under the chosen-ciphertext adversary. Thus, CP-ABE-CSSK offers constant size secret keysalong with efficient solution for encryption and decryption under the chosen ciphertext adversary, which supports an expressive AND gate access structure.

Aparna.V et al [5], in their workThe performance and security analyses was made efficient to securely manage the data distributed in the data sharing system. Attribute group keys are selectively distributed to the valid users in each attribute group, which then are used to re-encrypt the cipher text encrypted under the CP-ABE algorithm. The escrow problem was solved

John Burgess et al [6], in their work Disruption-tolerant networks (DTNs) attempt to route network messages via intermittently connected nodes.Routing in such environments is difficult because peers havelittle information about the state of the partitioned network and transfer opportunities between peers are of limited duration.In this paper, we propose MaxProp, a protocol for effectiverouting of DTN messages. MaxProp is based on prioritizing both the schedule of packets transmitted to other peers andthe schedule of packets to be dropped

3. METHODOLOGY

Constant Cipher text Policy Attribute-Based Encryption (CCCP-ABE)

In this section, we present CCCP-ABE scheme. The CCCP-ABE scheme consists of four fundamental algorithms:

- Setup (k)

The Setup algorithm takes input k as the number of attributes in the system. It returns public key KPU and master key KM. The public key is used for encryption while the master key is used for private key generation.

- KeyGen (KPU; KM; L)

The KeyGen algorithm takes the public key KPU, the master key KM and the user's attribute list L as input. It gives private key of the user as output.

- Encrypt (KPU; W; M)

The Encrypt algorithm takes the public key KPU, the specified access policy W and the message M as input. The algorithm outputs cipher text CT such that only a user with attribute list satisfying the access policy can decrypt the message. The cipher text also associates the access policy W.

- Decrypt (KPU; KPR; CT)

The Decrypt algorithm decrypts the cipher text when the user's attribute list satisfies the access policy specified in the cipher text. It takes the public key KPU, the private key KPR of the user and the cipher text CT as input. It returns the plaintext M if L j= W, where L is the user's attribute list and W is the access. So using CCP-ABE scheme, the cipher text can be abbreviated to a constant size even with increasing number of attributes.

Attribute-Based Broadcast Encryption

Based on CCCP-ABE, ABBE is flexible and efficient having cipher text is still constant in size. Compared to existing BE schemes, In ABBE, Encryptor does not need to store a large number of key materials, i.e., public key and private key. By carefully organizing the attributes in the system, the storage overhead of each user can be reduced from O (N) to
O (logN + m), where N is the number of users in the system and m<< N is the number of descriptive attributes in the system. Also in ABBE, an encryptor enjoys the flexibility of encrypting broadcast data using either a specific list of decryptors or an access policy without giving an exact list of decryptors. ABBE scheme facilitates flexibility of expressive access policy and efficiency of small Cipher text and public key. Moreover, any group member can encrypt/decrypt the message simultaneously to satisfy the many-to-many secure group communication requirements.

4. RESULTS

Welcome screen, login as administrator

Figure 2 Login screen

Figure 3 Home screen after Successful login.

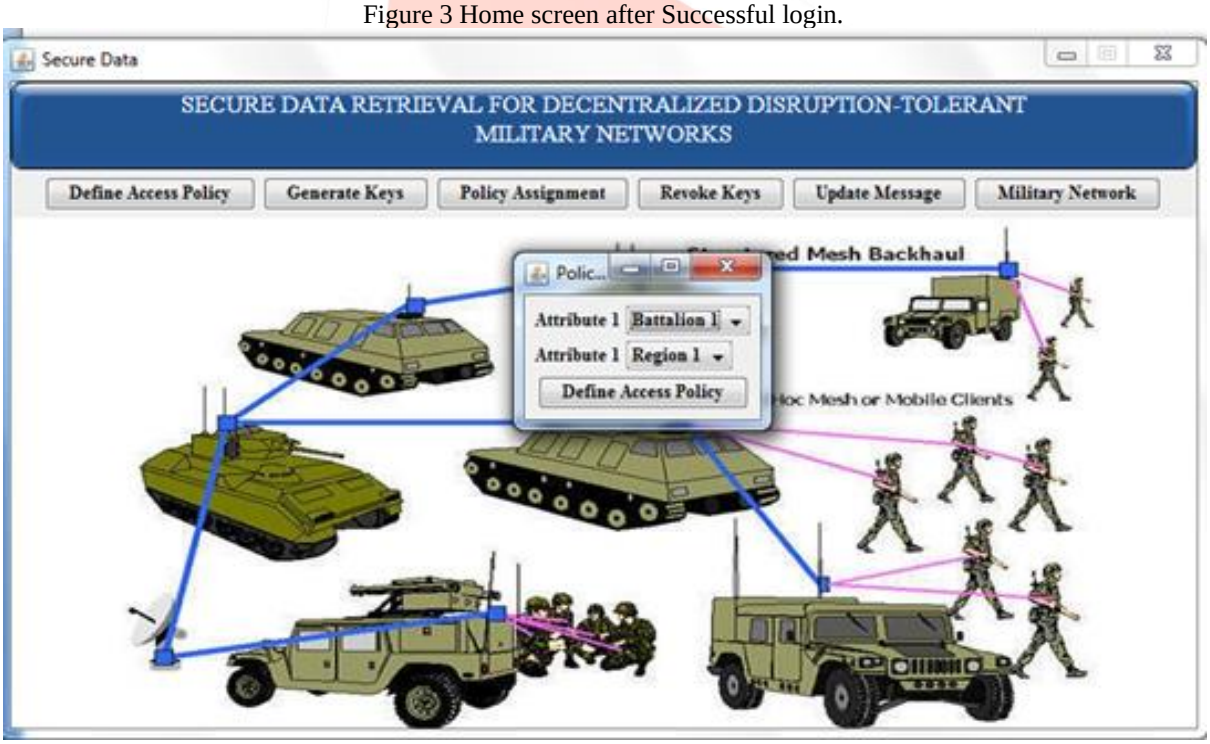

Figure 4 Create the access policy

Click on Define access policy you will find the screen as below. Here we are going to create Attributes (Nothing But for Battalion 1-Region 1 and click on Define access policy, Next Battalion 1-region 2, and click on Define access policy. In the same way Define access policy for all the Battalions)

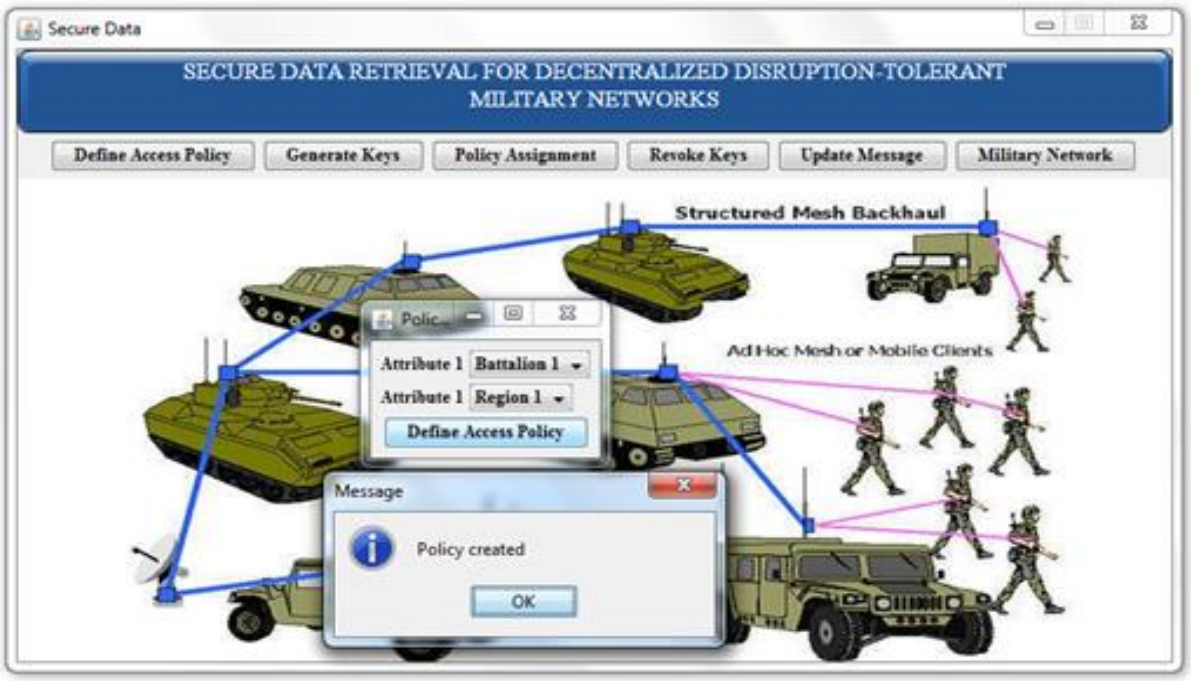

Figure 5 creating the policy for first set of attributes

In the same way create the policy for all the required attributes.
After Defining the access policy click on Generate Keys, to generate the keys for each set of attribute
Keys will be generated for every set of attributes and you can see the generated keys in the Key folder.

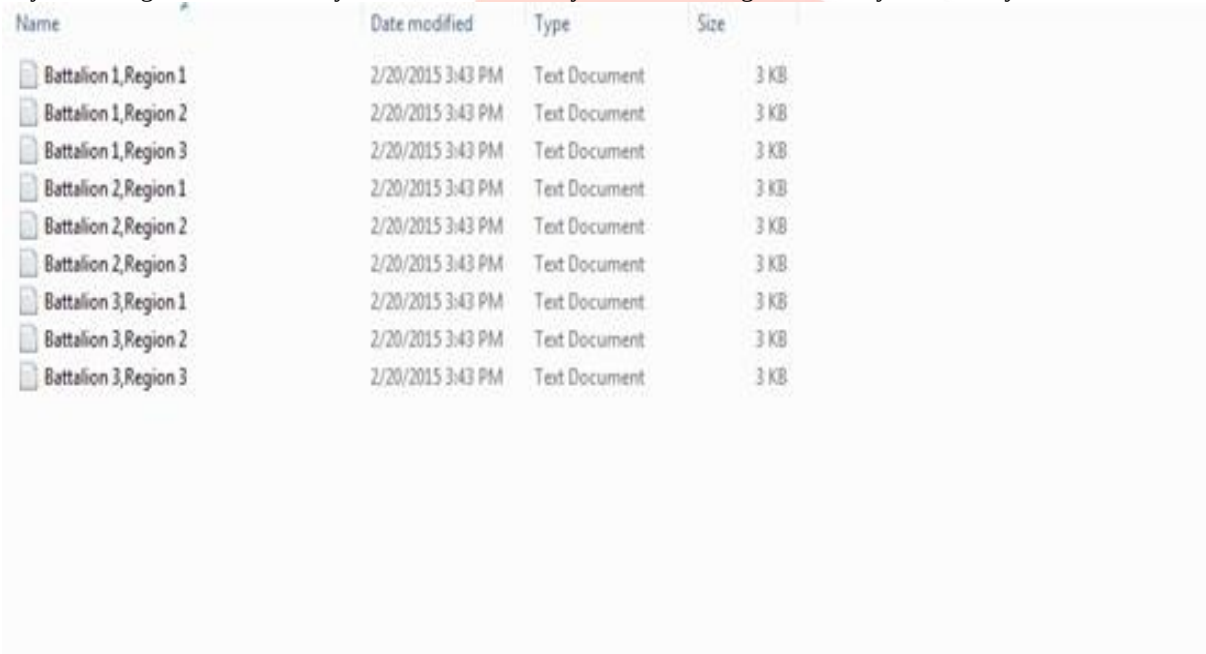

Figure 6 After generation of Keys

Policy Assignment:
In this Step we are going to assign policies for all the soldiers, to assign the policy click on Policy Assignment:
Policy assignment screen, in this soldier ID will be taken automatically and we need to give some policy for the selected soldier.

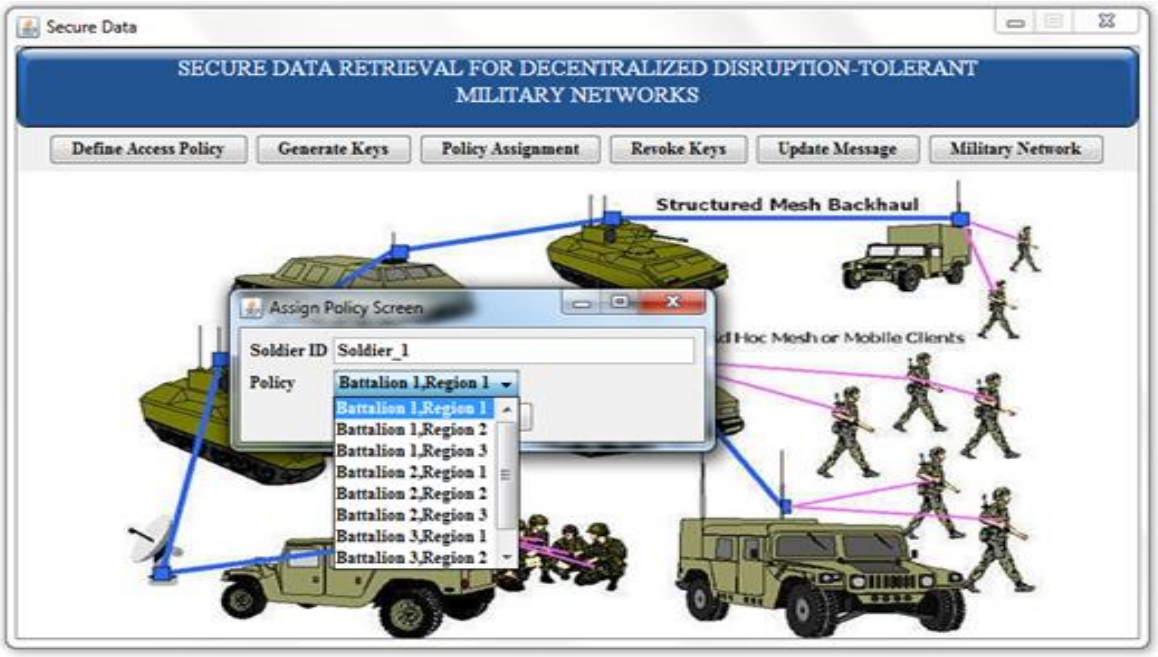

Figure 7 Policy assignment screen

Click on update message to send some message to particular battalion.

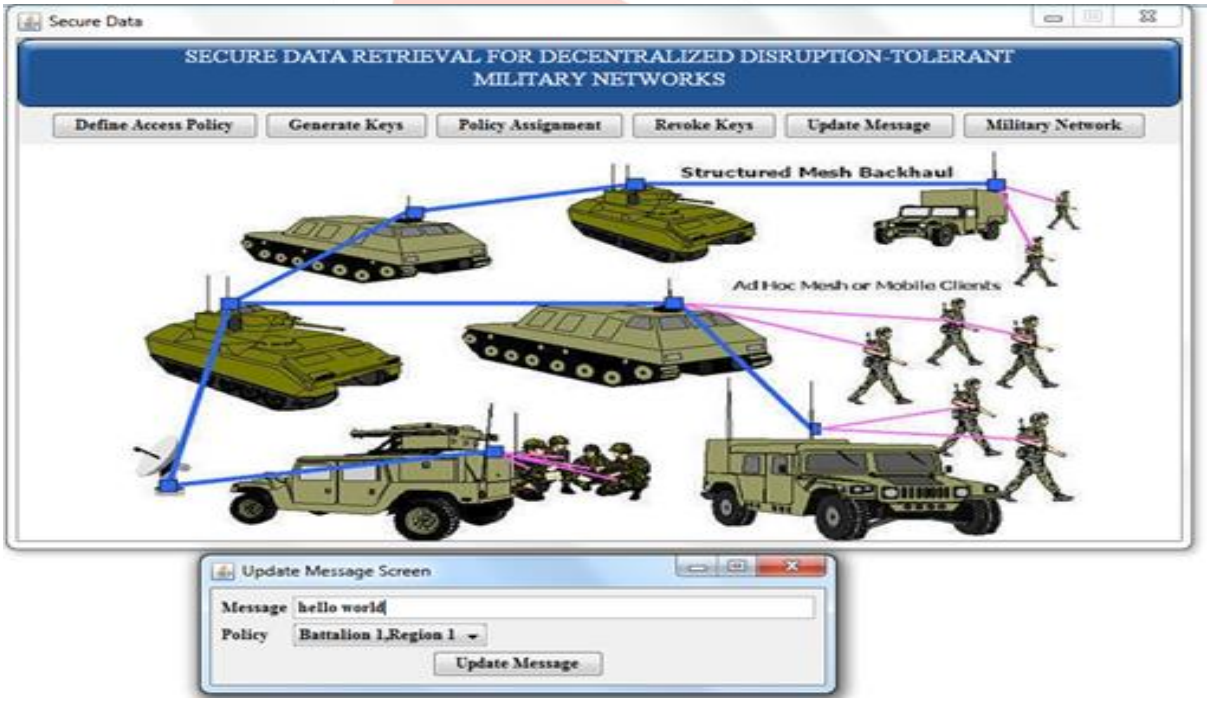

Figure 8 Update message screen

Enter the message and select some attribute:
Here we are updating the message ‘hello world’ and giving the accessibility for battalion 1 & region 1:

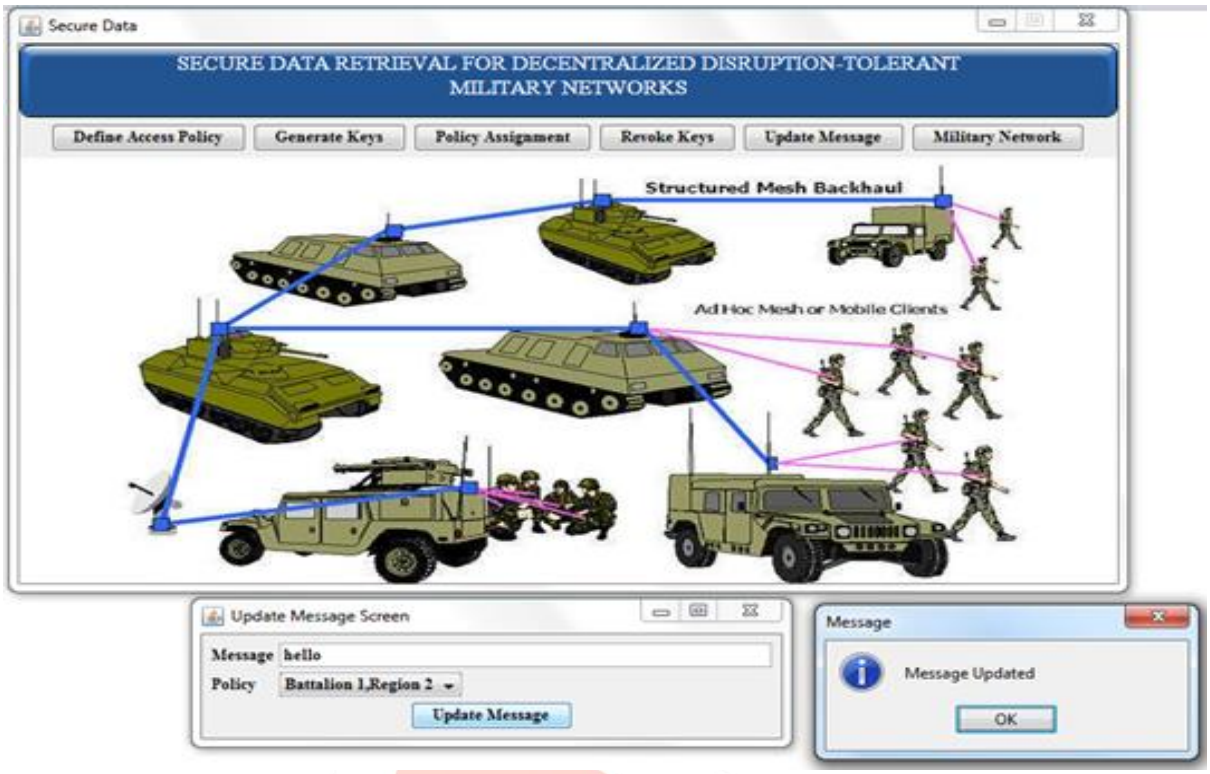

Figure 9 Updating a message 'hello' for battalion 1 & region

After updating the messages click on Military Network to see the network:

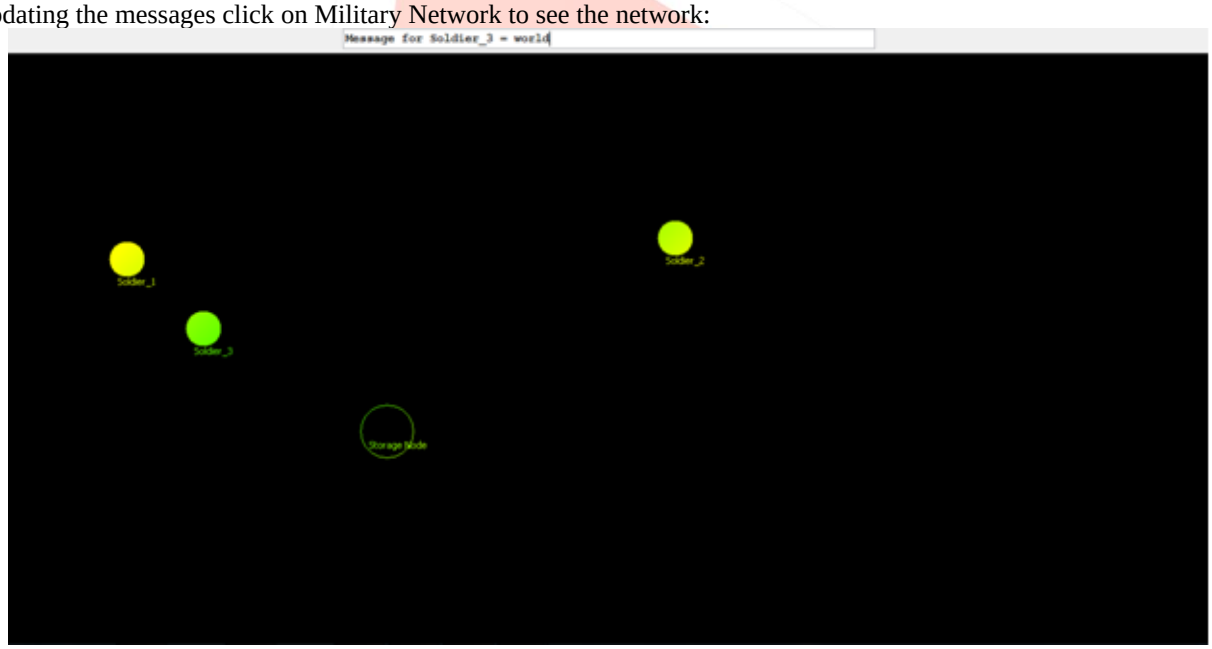

Figure 10 To See The Military Network.

In the above network, the storage node will store all the updated messages. The message which you updated in the update message step (I.e. message for the soldier-1, 2 or 3) will be displayed here when the particular soldier comes nearer to storage node.

Click on Revoke keys to revoke any key:

(We already assigned some soldiers to the specific battalions & regions, In this step we can move them from one region to another)

Moving soldier 3 from battalion 1 region 3 to battalion 2 regions1:

After moving:

Figure 11 after moving click on Military network

Here we moved node 3 from one region to another, so we don't have any key for this node.
So whenever the node comes nearer to storage node it can't access its data (shows no message for you)

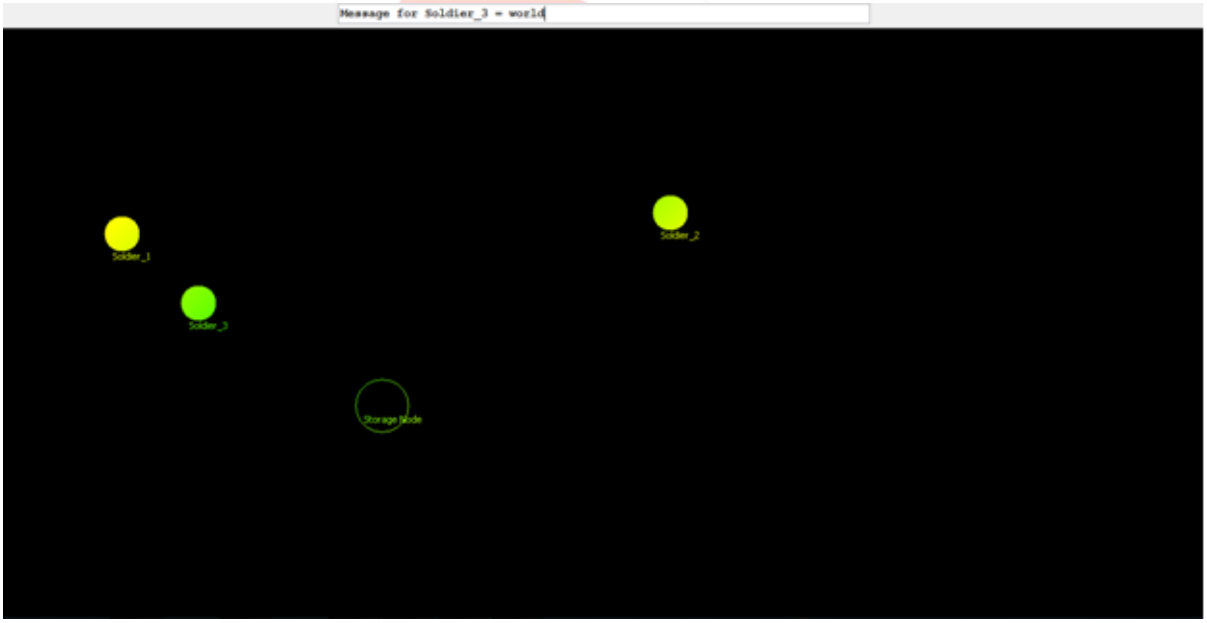

Figure 12 Military Network

5. Conclusion

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. 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 compromised or not 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] Vishal M. Shaha, Viral V. Kapadiab**, "** More efficient and flexible approach over traditional Cipher text Policy Attribute Based Encryption (CP-ABE) in form of Constant Cipher text Policy Attribute Based Encryption (CCP-ABE) and Attribute Based Broadcast Encryption (ABBE)",International Journal of Advanced Research in Computer Science and Software Engineering**,**Volume 4, Issue 7, 2014, pp.1133-1135.

[2] 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.

[3] S.Saranya , B.Suganya Devi, "A Novel AccessControl Mechanism to SecuretheDataDissemination in the DisruptionTolerant Network",*International Journal of Innovative Research in Computerand Communication Engineering***,**Vol. 3, Issue 2, February 2015,pp.1151-1156.

[4] VangaOdelu, Ashok Kumar Das, and AdrijitGoswami, "An Efficient CP-ABE with Constant Size Secret Keys using ECC for Lightweight Devices".

[5] Aparna.V, Jabisha Arul, Nandhini. S, Vishnu Kumar. A, "Multi Attribute Based Technique in Key Generation System", *International Journal of Engineering and Advanced Technology (IJAET), pp.614-617*

[6] Mooi-ChooChuah, Peng Yang, **"**Performance Evaluation of Node Density-Based Adaptive Routing Scheme forDisruption Tolerant Networks".