Securing Data Retrieval for Decentralized Disruption-Tolerant Military Networks (DTNs) using Cipher text-Policy Attribute-Based Encryption

Umoh Bassey Offiong[1], M. B. Mukeshkrishnan[2]

[1]*M.Tech Information Security and Cyber Forensics, Department of Information, Faculty of Engineering and Technology, SRM university Kattankulathur, India.*
[2]*Assistant Professor, Department of Information Technology Faculty of Engineering and Technology, SRM university Kattankulathur, India.*

Abstract:

DTN technologies are fast becoming popular and successful solutions in military applications that permit or enable wireless devices in the network to communicate with each other and access the confidential data infallible or in a trustworthy manner by utilizing the storage nodes. 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. The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over private and master keys, and cipher texts (CP-ABE). Scalability is provided by CP-ABE for data encryption and decryption. For decryption to take place the decryptor must possess some attributes that matches or corresponds with the one defined by security policy of the access control. We show how to apply the proposed scheme in securing and effectively manage the confidential data distribution in the DTN network.

KEYWORDS:- Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), secure data retrieval.

I. Introduction:

Military environment is a hostile and a turbulent one therefore, applications running in this environment needs more security to protect their data, access control and their cryptographic methods. For communication to take place a node must be created and a connection established between the node and the neighbour nodes in this hostile networking environment, but if there is no connection between the source and the destination the message from the source node may have to wait depending on when the connection will be eventually established. We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN. In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt.

The concept of attribute-based encryption (ABE) is a promising approach that fulfills 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. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. 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. 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. In order to realize the goals of CP-ABE the key authority makes use of maters secret keys and private keys of which the users apply by requesting it from the key authority. When a user keyed in some attributes that matches or corresponds with the one in the access policy, it is updated to match with the group attributes which provides security for group members.

II. Related Works

The concept of attribute-based encryption (ABE) 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. 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. 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 associated attribute 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.

III. Problem Definition:

Attribute Based Encryption poses some security and privacy problems to Disruption-Tolerant network (DTNs). Due to the fact that users in the network may change their associated attributes, master or private keys might be compromised. Therefore, in order to provide a secure system, key update is very necessary, but using ABE system the issue of secure system is more complex and difficult, since some attributes of each user are shared by multiple user in the network. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. The main disadvantages of this approach are efficiency and expressiveness of access.

IV. Existing System:

In existing system, the coordination of attributes issued from different authorities. When multiple authorities manage and issues 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. 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, or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems

Disadvantages of Existing System:

1. None of the authorities can determine the whole key components of users individually.
2. Failed to issuing key in decentralized.

V. Proposed System:

In this paper, we propose securing decentralized disruption-tolerant military networks (DTNs) using ciphertext-policy attribute-based encryption (CP-ABE). The proposed scheme The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over private and master keys, and cipher texts (CP-ABE). Scalability is provided by CP-ABE for data encryption and decryption. ABE enhances backward/forward secrecy of confidential data by

reducing the windows of vulnerability. Encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities.. We show how to apply the proposed scheme in securing and effectively manage the confidential data distribution in the DTN network.

Advantages of Proposed System:

1. vulnerability is minimized or reduced.
2. The Key Authority exploits the characteristic of the decentralized DTN architecture.
3. When once the new attributes of the group are updated the user cannot decrypt the nodes any
4. It provides scalability for data encryption and decryption.

System architecture:

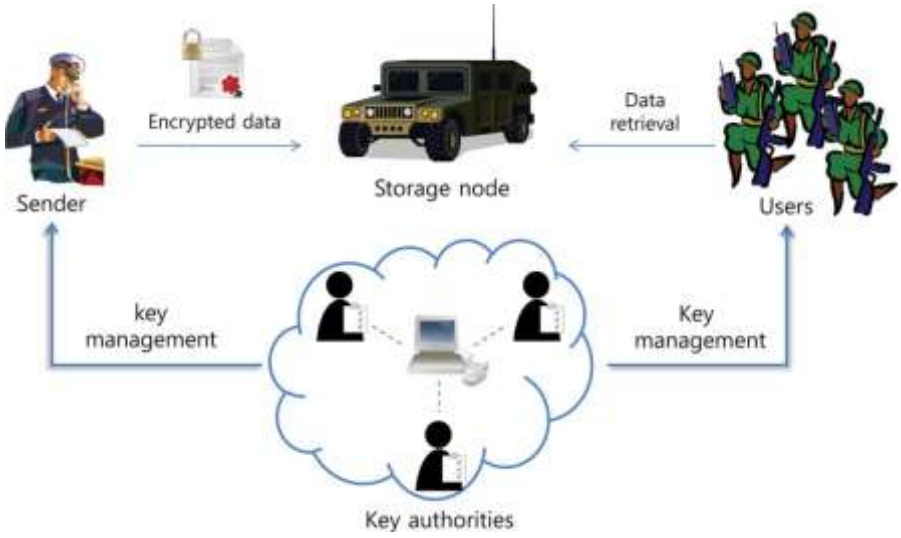

Fig. 1 System architecture of secure data retrieval in DTN

Data flow diagram

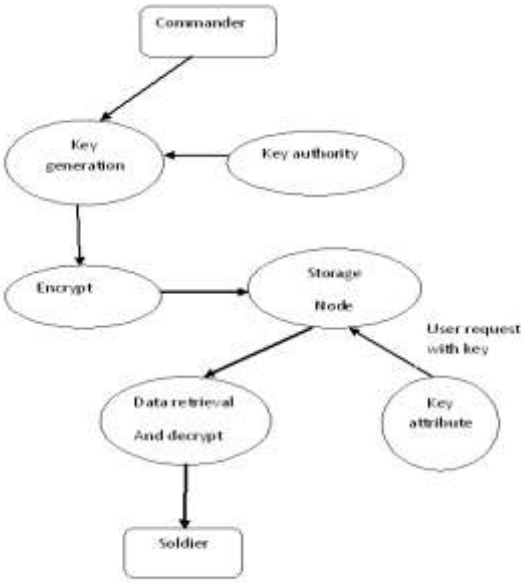

Fig. 2 Data flow diagram in DTN

VI. Implementation:

Implementation phase is a very important stage in the project execution. It is a phase or a stage where the theoretical aspect of the work is converted into a new and a working system. it is a stage where a user confidence is built up and is made to believe that the new system will work perfectly and effectively well. Therefore, it requires a careful planning, proper examination of the existing system and its problems, idea, model and design procedures to achieve the set objectives

Modules:

1. Disruption- tolerant network
2. Attribute-based encryption
3. Storage Nodes
4. Rekeying procedure

Fig. 3 Node creation with attributes in DTN

2. Attribute-based encryption:

The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over private and master keys, and cipher texts (CP-ABE). Scalability is provided by CP-ABE for data encryption and decryption. For decryption to take place the decryptor must possess some attributes that matches or corresponds with the one defined by security policy of the access control.

Modules description:

1. Disruption tolerant network:

Disruption tolerant network is a network that allow creation of node and neighbour nodes and permit communication between nodes in these hostile and turbulent networking environments. For communication to take place a node must be created and a connection established between nodes in the networking environment, but if there is no connection between the source and the destination the message from the source node may have to wait depending on when the connection will be eventually established. There are multiple paths in DTN network, the storage in DTN is use to store, mange and also for forwarding using the shortage paths in the form of weight. Finally, it introduces storage nodes for storing information.

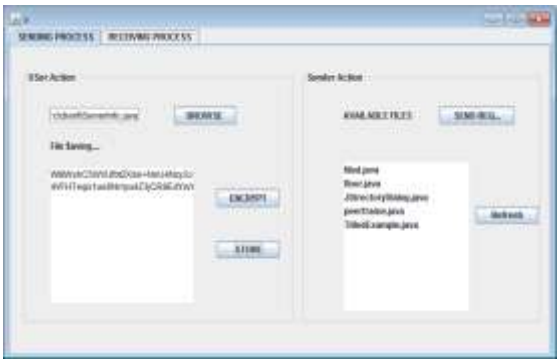

Fig. 4 Showing how a file is encrypted

3. Storage nodes:

In DTNs, storage node is where data is stored, managed and duplicated for effective communication and quick access to information by the authorized mobile nodes in the network. 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 securely. Sender can define the access policy under attributes of any chosen set of multiple authorities without any restrictions on the logic

expressiveness as opposed to the previous multi authority schemes.

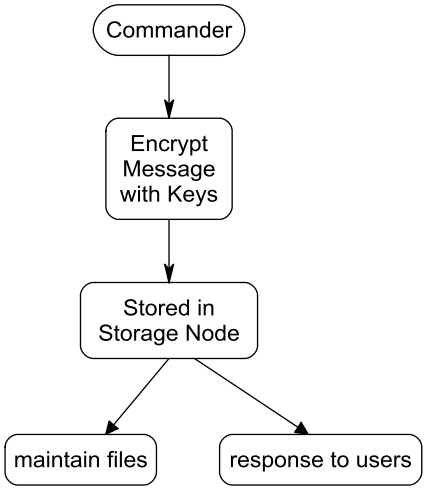

Fig.5 Data flow in Storage module

Fig.6 Storage screen in DTN network.

4. Rekeying:

The purpose of rekeying is to provide security to the system. It is impossible to revoke specific attribute keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. But it seems very ineffectual and may serious complexity terms of the computation and communication cost, especially in large-scaled DTNs.

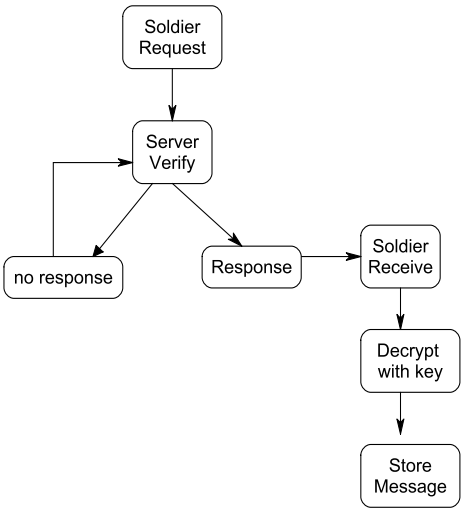

Fig.7 rekeying data structure

System Requirements:

Software Requirements:

- Front End : Java
- Environment : Eclipse Indigo
- Back End : MYSQL
- Operating System: Windows XP/7

Hardware Requirements:

- Processor : Pentium IV 2.4GHZ
- RAM : 512 MB
- Hard Disk : 80 GB
- Monitor : 15 VGA colour

VI. Conclusion:

DTN technologies are fast becoming popular and successful solutions in military applications that permit or enable wireless devices in the network to communicate with each other and access the confidential data infallible or in a trustworthy manner by utilizing the storage nodes. The ABE scheme provides access controls mechanism over an encrypted data with its policies and attributes over

private and master keys, and cipher texts (CP-ABE). Scalability is provided by CP-ABE for data encryption and decryption. In this paper, we proposed an efficient and effective way for securing data using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. In order to realize the goals of CP-ABE the key authority make use of mater secret and private keys of which the users apply by requesting it from the key authority. When a user keyed in some attributes that matches or corresponds with the one in the access policy, it is updated to match with the group attributes which provides security for group members. We show how to apply the proposed scheme in securing and effectively manage the confidential data distribution in the DTN network.

VIII. Future Work:

Besides, we plan to investigate the feasibility of incorporating value compare predicates
in policy tree in the future so that the sender can control the lifetime of attributes.

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

[4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7. [6] M. Kallahalla, E. Riedel, R.

[6] Swaminathan, Q. Wang, and K. Fu,"Plutus: Scalable secure file sharing on untrusted storage," in *Proc.Conf. File Storage Technol.*, 2003, pp. 29–42.

[7] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in *Proc. WISA*, 2009, LNCS 5932, pp. 309–323.

[8] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in *Proc. Ad Hoc Netw. Workshop*, 2010, pp. 1–8.

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," *Ad Hoc Netw.*, vol. 7, no. 8, pp. 1526–1535, 2009.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

[11] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 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] Battu Hanumantha Rao, K.Padmaja ,P.Gurulingam "A Brief View of Model Based Systems Engineering Methodologies" *International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue8- August 2013.*

[14] Mohit Taneja, Sandeep Nandal, Arpan Manchanda, Ajay Kumar Agarwal " Experimental Study of Convective Heat Transfer and Thermal Performance in the Heat-Sink Channel with Various Geometrical Configurations Fins" International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 6 – June 2013.