Efficient Data Flow Analysis of Disruption Tolerant Networks Using Encrypted Technique

Satheesh. M[1], Nancy. X[2]
Assistant Professor, Department of Computer Science, Arjun college of Technology, Coimbatore

Abstract: ***An efficient system for protecting the Confidential news and location leaks in Sensor Networks and also secures the privacy-preserving scheme against traffic analysis and flow tracing. The attribute-based encryption is a approach that fulfills the requirements for secure data retrieval using access policies among private keys and ciphertexts in Disruption-tolerant networks. Disruption-tolerant network (DTN) is now emerging as an efficient method that allow wireless devices carried by soldiers to communicate with each other and access the secret messages or command reliably by exploiting external storage nodes. Few of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Mobile nodes, in certain applications, the location of the node tracked by sensor networks need to remain anonymous. That is, unauthorized observers must be unable to detect the origin of such nodes by analyzing the network traffic. With the help of homomorphic encryption algorithm technique, the scheme offers two significant advantages, packet flow untraceability and message content confidentiality, that perfectly detects the flow tracing attacks and traffic analysis. The proposed system demonstrates how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant network.***

Keywords: Disruption Tolerant Network (DTN), Attribute Based Encryption (ABE), Ciphertext-Policy Attribute Based Encryption (CP-ABE), Key-policy Attribute Based Encryption (KP-ABE), Key escrow, Attribute Revocation.

I. INTRODUCTION

Networking is the link between two or more computers and their devices, whose main need is sharing the data stored in the computers, with each other. Communication is done by means of either wired or wireless devices. Military is an area where soldiers will mainly rely on wireless mobile devices for communication. Connection between these wireless devices sometimes may or may not get connected because of environmental issues or the mobility. In such communication between soldiers doesn't occur.

Disruption Tolerant Network (DTN) is one technology where it makes possible of communication when there is no peer to peer connection between the wireless devices. In the DTN technology the message from source to destination will be stored in one intermediate node when there is destruction in the path between source and destination. Data in military application are confidential ones. These data's must only be accessed by authorized groups of user and unauthorized users must be denied from access.

In cryptographic methods having different access policies for different users. So that only those users with correct access policies can access the particular data. Thus these methods facilitate secured retrieval of the information. Recently Ciphertext Policy Attributed Based Encryption in decentralized DTNs has been introduced. But this scheme faced many security related problems like Key escrow, Attribute revocation and Coordination of attributes are issued from different authorities. To solve these problem, Multi-authority CP-ABE scheme has been proposed. Here local authority issues attributes for the user by performing secure 2PC protocol with central authority. Hence users attribute key can be updated individually.

II. RELATED WORKS

Mobile Nodes in some critical network scenarios suffers intermittent connectivity and frequent partitions. Several application scenarios require a security design that provides fine grain access control for the informations stored in storage nodes within a DTN or to contents of the messages routed through the network .The Ciphertext Policy Attributed-Based Encryption (CP-ABE) provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. ABE comes in two flavors called key-policy ABE(KP-ABE) and ciphertext-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. In CP-ABE, the ciphertext is encrypted with an access

policy chosenby an encryptor, but a key is simply created with respect to an attributes set

A. Attribute Revocation*:* Bethencourt et al. [13] and Boldyreva et al.[16] suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append each attribute an expiration date (or time) and distribute a new set of keys only to the valid users after the expiration. ABE schemes have two main problems,(a) security degradation in backward and forward secrecy,(b) scalability problem.

1) *Key Escrow:* Chaseetal.[24] presented a distributed KP-ABE scheme that solves the key escrow problem in a multi-authority system.In all(disjoint) attribute authorities are participating in the key generation protocol in done in a distributed way such that they cannot gather their data and link multiple attribute sets belonging to the same user. One disadvantage of this fully distributed way is the performance loss. Since there is no common authority to master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key.

2) Decentralized ABE: Huang et al. [9] and Roy et al. [4] proposed decentralized CP-ABE schemes in the multi-authority network environment. They achieved a combined access policy over the attributes issued from various authorities by just encrypting data multiple times. The main disadvantages of this approach are efficiency and expressiveness of access policy.

III. SYSTEM ARCHITECTURE

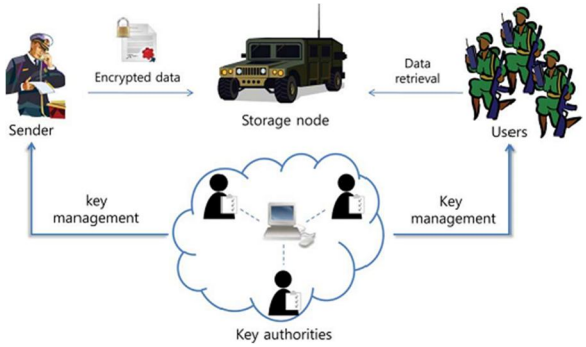

Fig. 1. Architecture of efficient data flow analysis of disruption tolerant networks using encrypted technique.

A. System Description

The architecture contains the below system entities.

1) Key Authorities: They are the key production/generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and many local authorities. We assume that there is a secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each and every 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 assummed 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 the encrypted content 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 mo- bile 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 messages or 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 that wants to access the data in 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 the ciphertext and obtain the data.

B. Threat Model And Security Requirements

1) *Data confidentiality:* Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node.

2) *Collusion-resistance*: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone [11]–[13]
3) *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 predecessive 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 successive data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

IV. PROPOSED SCHEME

The proposed procedure depends on multi-authority CP-ABE instrument for secure information gathering in DTNs. There are two key issuing powers' to be specific expert key power and the nearby key issue power. Expert power issues the keys to nearby power and it to its client. The clients need to decode the information through qualities issued by its concerned power. Scaliblity and security are accomplished in proposed idea with usage of element quality overhaul.

Access Structure: Here we assume a set of parties {P1, P2, P3 …. Pn} and a is a monotone if if⊆C and . where is a nonempty subset {P1, P2, P3….Pn}. so the in are authorized sets and set not in are unauthorized sets. In proposed scheme the attributes take the role of parties. So an monotype structure is known as access structure.

Bilinear pairings: Let 0 and 1 be two multiplicative cyclic group of prime order p. Let g be generator of 0. A bilinear map is defines as e: 0 x 1 1. If e(Pa, Q b) = e(P,Q)abfor all P, Q 0 for all a, b * P.

A. *Scheme Development*

To construct the system we need to undergo different steps as below

1) *System setup:* In this phase every trusted initializer selects a bilinear map 0 which has a prime order of p with generator g based on security parameters. A universal one way Hash function is selected.
2) *Central key authority:* It generates the public/private key pair and issues to the local key authorities.
3) *Local Key authorities:* After receiving the public/private key pair from CA key authority, it is transferred to concern user.
4) *Key Generation:* In existing approach CP-ABE it consist of many attribute keys and one personalized key. To overcome the collusion attack different and unique personalized key is generated for every user.

B. *Personal/unique Key Generation Protocol*

The personal key authority and local key authority are responsible in generation of personal key for a user.

C. *Algorithm Unique key generation*

1) Step 1: CA communicates with user and authenticates it. Every user is assigned with a unique random exponent with respect to every local authority. With the above values it generates rt value for every local authority L1, L2, L3…..Ln L. This rt value is unique and secret to the user.

2) Step 2: Local authority Li randomly picks and computes T value and sends it to CA. Step 3: CA then computes M value and sends it to the Li.

3) Step 4: Li results a unique key component Fi and sends it to the user Ut. User then computes its personal key for encryption.

4) Encryption: When a sender wishes to send some confidential data to the receiver he selects a appropriate encryption algorithm and uses the attributes generated by the central authority and issued by local authority.

5) Decryption: When receiver receives the cipertext Cp from storage node it uses the attribute M generated by local authority Li and uses its unique key and decrypts the cipher tectcp to plaintext. An efficient decryption algorithm is used by decryptor.

V. CONCLUSION

In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key

authorities monitor and 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 com- promised or not fully trusted. A statistical framework based on binary hypothesis testing for modeling, analyzing, and computing statistical source anonymity in wireless sensor networks. we showed why previous studies were unable to detect the source of information leakage that was demonstrated and explained in this paper. Finally, we have proposed a modification to the existing solutions to improve their anonymity against correlation tests.

REFERENCES

[1] Burgess J(2006)., 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] Chen N.,(2010) 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.
[3] Chuah M.(2007) and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.
[4] Lewko A(2010). and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.
[5] Tariq M.(2006) M. B., 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.
[6] Chuah M.(2006) and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp. 1–6.