International Journal of Science Engineering and Advance Technology

A System for Secured Data Retrieval in Hostile Regions using CP-ABE Based in Ad Hoc Disruption- Tolerant Networks

A.Radhika, D. VaraLaxmi
[1]Sr.Asst.Professor, Dept. of CSE
[2]M.Tech(CS),Dept. of CSE, S.R.K Instt. Of Technology Andhra Pradesh, INDIA.

Abstract-Generally Networks operated in ad hoc mode suffer isolated network connectivity in the Hostile Military environments like battlefield. Deployment of Disruption-tolerant networks (DTN) enhances the connectivity between wireless devices carried by soldiers in battle field, this provides them to communicate effectively and share the information confidently. Cipertext -policy attribute based encryption (CP-ABE) is effective cryptographic technique to access control issues. Ad hoc network are decentralized and resource constrained networks, applying CP-ABE to such networks is a challenging issue, in turn it introduces new security and privacy issues related to attribute revocation, coordination of attributes, and key escrow. This paper mainly focuses on a secure data collection mechanism using CP-ABE for ad hoc DTNs where more than one key authority manages their attributes dynamically and independently. We analyzed the proposed mechanism and applied to the disruption-tolerant military network to access the information securely.

Keywords: DTNs, CP-ABE, Ad hoc Network, Key Management.

I. Introduction

In many Military scenarios, military communication networks are decentralized by nature and connected via wireless devices carried by soldier, due to some environmental factors, and mobility they are disconnected, and jammed. To overcome researchers are finding new technologies like Disruption-tolerant network (DTN), these networks allows nodes to communicate in distinct environment conditions [2]–[3]. In multi hop ad hocnetworks data should be forwarded via intermediate nodes, the data should be stored at these nodes should be retrieved securely until the connection is established between source and destination. An approach of storage of data at nodes which can be accessed only by authorized nodes was proposed by Chuah [4] and Roy [5]. Confidentiality and integrity should be maintained in military application by applying cryptographic techniques [6]. Based on ad hoc network and hostile network features it is required to define new data policies based on user attributes and roles managed by different key management authorities. In real time DTNs can be used in military communication where a commander can store and forward the data to particular battalion and the only specified battalion can retrieve the data securely later. In DTN architecture show in fig 1 we can observe that multiple authorities can issue and manage their own attribute key in the absence of centralized authority [7]. Beside many encryption techniques attribute based encryption best suit for DTNs for secure data collection. The main feature of ABE is it provides access control over data based on access policies and qualified attributes among cipher texts and user private keys [8]-[10]. CP-ABE is a scalable approach for encryption of data where encryptor defines the attribute set which decryptor uses to decrypt the message. So based on the security policy different users are allowed to decrypt different pieces of data [10].

The major issue with ABE is applying this mechanism to DTNs which are decentralized, in the process it may lead to several privacy and security issues. In military networks due to mobility of nodes (battalion from one region to other) may compromise users private keys, the alternate to this is key revocation for every attribute through which it may achieve security. The new problem is these keys should generate whenever a node moves from one region to another. The other challenge is key escrow problem. Every key authority has a master secret key through which all user data can be decrypted, in case of key authority compromised by attackers in military communication network. This will be serious threat for security and data confidentiality. Finally

coordination of attributes issues by different key authorities.

II. Related Work

There are two flavors of Attribute Based Encryption (ABE) namely Key-policy ABE(KP-ABE) and ciphertext-policy (CP-ABE). The main problem with KP-ABE is, only the encryptor gets the label to cipher text with some attribute set and the key authority maintains some access policies which are embedded in key issues to the user. This key can be used by the receiver to decrypt the message. These roles are reversed in CP-ABE, the cipertexts is encrypted with an access policy by encryptor and key is created by a set of attributes. So CP-ABE is more flexible for DTNs compared to KP-ABE [4][11].

Some work has done on CP-ABE and KP-ABE regarding key revocation mechanism by and*Boldyreva et al and* Bethencourt*et al* [9]. But their solution has a limited validity of keys and after expiration date or time new certificates should be issues to valid user. These periodic attribute recoverable ABE schemes have two major problems.

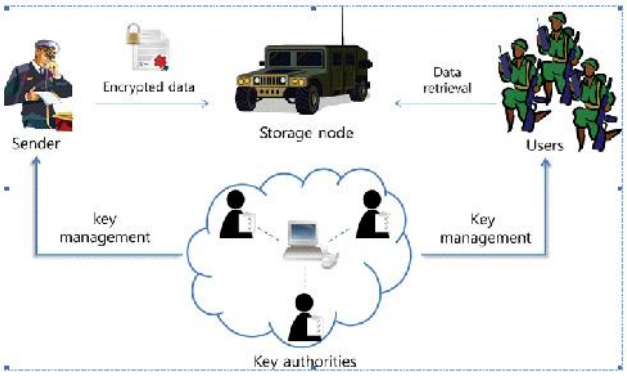
The first is problem regarding security degradation i.e forward and backward secrecy and the other is scalability problem.Golle*et al.*[12]proposed a user revocable KP-ABE mechanism, the major flaw of this scheme is it operates only if no of attributes are half of the universe size.

Chase et al proposed a distributed KP-ABE that provide solution for key escrow problem in multi authority system. The communication overhead of this is scheme is $O(N^2)$ where N is the no of authorities in system.

Huang et al. proposed a decentralized ABE scheme in multi authority environment. It achieved a combined access policy over attributes issued by various authorities by simple encryption algorithm.

III. System Architecture

The basic DTN architecture is define in Fig 1. Which can be used in DTNs based military network.



The system architecture shown in Fig. 1 has the following aspects.

3.1 Sender: This is where the data transmission begins with encryption of data in real time it may represent a commander who sends the data to its battalion located in different regions. Sender node is only responsible to encrypt the data using its own access policies.

3.2 Storage Node: It is intermediate node which stores the data and provide access to the data when the user is available. Storage node may be static or mobile. This node can also be compromised since it is a semi trusted.

3.3 Key Authorities: these authorities generate the keys for both encryption and decryption in CP-ABE. It is a combination of central and local authorities. we need to assume that there is secure and reliable data channel between both the authorities during initial key generation and sharing. The user communicates dto local authority which validates user and issues attributes to the users. Users get access based upon the user attribute values.

3.4 Receiver/User: receiver (soldier) node can access the information from the storage node (intermediate node) which is transferred by sender node (commander). User need to satisfy all the access policy of encrypted data to decrypt the cipher text.

3.5 Security Architecture: To achieve forward and backward secrecy, data confidentiality and collusion-resistance security architecture is defined as below.

3.6 Backward and forward Secrecy: backward secrecy means the user need only to access the information after holding the attribute issues by key authority, the previous data cant be accessed. Forward secrecy means once the user drops attribute he should not be able to

access the cipher text until unless the attribute he holding satisfy the key agreement.

3.7 Data confidentiality: there should be a mechanism where unauthorized users holding access policy should not access the cipher text. It should be prevented and for both user and key authorities.

3.8 Collusion-resistance: multiple users can combine their attributes in case of a single user cant decrypt the message. This may lead to collusion attack, so we need to implement a mechanism so that no two nodes can combine their attributes to decrypt the message.

3.9 Technical Terminology :We propose some basic definition regarding proposed scheme, mainly access structure to define definitions and bi linear map and its security requirements. [12][13]

3.10 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 of p. Let g be generator of $_{0.}$ A bilinear map is defines as e: $_0$ x $_1$ $_{1.}$ If e($P^{a,}$ Q^{b}) = $e(P,Q)^{ab}$for all P, Q $_0$ for all a, b * $_{P.}$

IV. Proposed Scheme

The proposed technique is based on multiauthority CP-ABE mechanism for secure data collection in DTNs. There are two key issuing authorities' namely master key authority and local key issue authority. Master authority issues the keys to local authority and it to its user. The users need to decrypt the data through attributes issued by its concerned authority. Scaliblity and and security are achieved in proposed scheme with implementation of dynamic attribute update. Based on first CP-ABE proposed by Bethencourt*et al.* [13]

Bethencourt*et al.* [9], many of CP-ABE schemes have been proposed [12]–[15]. All these schemes are based on Bethencourt*et al.*'s scheme, but failed to achieve the declarations and terminology. Proofs of those schemes are analyzed but not many simulated. Proposed technique is based Bethencourt*et al.*'s construction in order to enhance the expressiveness. It has four modules as below

4.1 Access Tree :

- Description: For a tree be representing access structure. A threshold gate is maintained for every non leaf node. If a tree x has num_x no of children's then $k_x$is its threshold value then0 $k_x$$num_{x.}$ an attribute is defined for every leaf node and the threshold value is $k_{x\,=}$ 1.
- Fulfilling an Access Tree: Every tree is having a sub tree at some node. Let has a sub tree at node x which is $_{x.}$ we can calculate $_x$ () = 1. Where α is a set of attributes. We can compute $_x$(α) recursively.

4.2 Scheme Development:

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

4.2.1 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.

4.2.2 Central key authority: It generates the public/private key pair and issues to the local key authorities.

4.2.3 Local Key authorities: After receiving the public/private key pair from CA key authority, it is transferred to concern user.

4.2.4 Key Generation: In existing approach CP-ABE it consist of multiple attribute keys and single personalized key. To overcome the collusion attack different and unique personalized key is generated for every user. A separate approach for generation of personal key is composed in proposed solution.

Personal/unique Key Generation Protocol:

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

Algorithm Unique key generation:

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 $r_{t\ value}$ for every local authority L1, L2, L3…..Ln L. This $r_{t\ value}$ is unique and secret to the user.
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.
Step 4: Li results a unique key component Fi and sends it to the user Ut.
User then computes its personal key for encryption.

Attribute Key: Attribute keys are generated by the local authority Li once the unique key component is generated.

Algorithm for attribute generation:

Step 1: CA picks a random value and generates attribute r' and sends it to Li and user.
Step 2: Li takes set of attributes generated by CA and generates keys for user and transfer rj to each user.

- 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.

- Decrypt: When receiver receives the ciper text 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.

Revocation: whenever a key is changed by the user then all the local authorities should be updated with the newly assigned key which is generated by the CA. problem with this mechanism is that it may generate more overhead in terms of computation and communication cost. The alternate to this problem is to re-encrypt the attribute value and validate it and share it with local authorities and user.

V. Analysis:

The proposed technique is compared with the existing CP-ABE schemes and it shows that the poposed algorithm is dynamic in terms of all the phases of Cp-Abe than others.

Table 1 comparative analysis of CP-ABE for DTN with other approaches.

Scheme	Authority	Revocation	Keyescrow
BSW	Single	Periodic attribute	yes
HV	Multiple	Periodic attribute	yes
RC	Multiple	Immediate system-level	yes
proposed	Multiple	Immediate attribute-level	no

VI. Conclusion

DTN based communication networks are becoming more popular ad hoc networks and are being deployed in military applications to allows wireless ad hoc device to communicate efficiently. Information should be reliably transmitted between the sender and receiver, so key management plays a vital role in providing data confidentiality and privacy. CP-ABE based solutions are very scalable compared to other cryptographic approaches. In this paper we proposed an efficient and scalable CP-ABE based approach which can be used for secure data collection in military communication networks that operate on DTN technologies.

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. 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.

5. 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.

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

7. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. Eurocrypt, 2005, pp. 457–473.

8. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Proc. IEEE Symp.Security Privacy, 2007, pp.321–334.

9.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.

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

11. S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," Comput.Surv., vol. 35, no. 3, pp. 309–329, 2003.

12. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security, 2007, pp. 456–465.

13. V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp. 579–591.

14. X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in Proc. ASIACCS, 2009, pp. 343–352.

AUTHOR'S BIOGRAPHY

Mrs.A.RADHIKA, well known Author and excellent teacher Received M.Tech from JNTU Kakinada, She is presently working as Sr. Assistant Professor, Department of CSE, S.R.K Institute Of Technology. She has 15years of teaching experience in engineering colleges. To her credit she has couple of publications both national and international conferences journals. Her area of interest includes Computer networks, Manets, Security in Manets, Information Security.

Mrs.D.VaraLaxmi is a student of S.R.K Institute Of technology, Enikepadu. Presently she is pursuing her M.Tech[Computer Science Engineering] from this college and she received her M.Sc. degree from P.B Siddhartha College of Arts and Science affiliated to Krishna University, Machilipatnam in the year 2012.Her area of interest includes Computer Networks, Security Concepts and all current trends and techniques in Computer Science.