ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 12, December 2017

Disruption Tolerant Networks using CP-ABE for Military Applications

Diddi Srilatha, BVSP Pawan Kumar

***Abstract*— In military environments, nodes suffer from intermittent connectivity of network and frequency variations in partitions. The ultimate resolution to this issue is solving by Disruption-Tolerant Network (DTN) providing a friendly environment to communicate among themselves and share confidential information via wireless devices. To maintain confidentiality and reliability in this scenario is mandatory to update policies for data retrieval securely. The policies of authorization can be enforced using Ciphertext-Policy Attribute-based Encryption (CP-ABE). The later implementation of CP-ABE can lead to severe privacy and security complications with regard to key escrow attribute revocation and attributes coordination issued by various authorities. In this area of research, we suggested an efficient data retrieval scheme which is more secure for decentralized DTNs. The secure data retrieval is manageable for independent attributes with multiple key authorities. We also demonstrated how the suggested mechanism is applicable to manage efficient and secure distribution of data confidentially in disruption tolerant military networks.**

***Index Terms*— Ciphertext-Policy Attribute Based Encryption, Data Confidentiality, Decentralized CP-ABE, Decentralized DTNs, Disruption-Tolerant Network.**

I. INTRODUCTION

The connections established by soldiers in military networks are through wireless devices. These connections may be disconnected temporarily by environmental factors, jamming and mobility especially in hostile environments. Technologies like Disruption Tolerant Networks are becoming more successful by allowing the nodes to communication together in these networking environments extremely. More typical, the source node during the time of data access the messages has to wait in the intermediate node for some time until the connection is established eventually in the non-presence of node-to-node connection between the source pair and destination pair. Chuah and Roy has introduced DTN based storage nodes where the data is replicated in such a way that only authorized remote nodes can access information needed a high speed and efficiency. Most of the military technology applications need an increased protection of data confidentiality which must include control methods to access and enforced the same cryptographically. In most of the cases, it is necessary to provide variations in access services so that policies to access data are defined over user roles or attributes and are handled by numerous key authorities. We in this paper refer to the conventional architecture called Disruption Tolerant Network architecture where numerous authorities can manage and issue their attribute keys as decentralized independently.

The attribute-based encryption (ABE) concept is an approach that fulfills data retrieval requirements securely in DTNs. The ABE facility can enables a control over the access of encrypted data by using policies and attributes among the private keys and encrypted text. Especially CP-ABE provides a way to encrypt data so that encryptor defines the set of attributes that are needed to decrypt in order to obtain the decrypted text.

However, the application of CP-ABE to disruption tolerant networks can introduce various privacy and security challenges. Key renovation or update for every attribute is mandatory to make systems secure because many of the users may modify their associated attributes at their moving region or few private keys may be compromised. This means that the revocation of some single user or attribute in a group may affect the attributes associated redistributed or changed to all other associated members in a group.

For example, if any of the users newly joins or leaves from an attribute group, then an associated attribute key typically be redistributed and changed to all the associated members in the related group for forward and backward secrecy. It also result in bottleneck during the procedure of rekeying or degradation of security due to the late updating of the existing attribute key immediately.

II. RELATED WORK

CP-ABE can be implemented in two methods named Key Policy ABE and Cipher Text Policy ABE. In key policy ABE, an encryptor gets to label an encrypted text with a collection of attributes. A policy was chosen by key authority to determine for user which encrypted text the user may decrypt and simultaneously can issue the key with an embedded policy into each user's key. To avoid complexity the keys and the encrypted text roles has been revised in CP-ABE. The encrypted text is created based on the access policy chosen with respect of attributes set. Key-Policy ABE enables

***Diddi Srilatha**, M.Tech Student, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisamma Guda, Dulapally, Secunderabad, Telangana, India.*

***BVSP Pawan Kumar**, Assistant Professor, Department of Computer Science and Engineering, Malla Reddy Engineering College for Women, Maisamma Guda, Dulapally, Secunderabad, Telangana, India.*

encryptor like commander to select certain policy of access and to encrypt more confidential data in view of access structure via related public keys encryption.

A. *Attribute Revocation*

Boldyreva and Bethencourt suggested first key revocation implementation in Cipertext Policy-ABE and Key-Policy ABE. Their solutions append each attribute a date of expiration and after expiration distribute a new pair of keys to verify users.

B. *Key Escrow*

Many of the ABE schemes are developed based on an architecture where an individual trusted authority has the efficiency to generate user's private keys with its non-dependent secret information. Thus, the problem of key escrow is inherent so that the secret key generation in the system can decrypt every encrypted text addressed at any time to users.

C. *Decentralized ABE*

Roy and Huang suggested CP-ABE decentralized schemes in the network environment with multiple authorities. Over the issued attributes, they have achieved a combined policy of access from several authorities by data encryption data multiple number of times. The main drawbacks of this method are access policy expressiveness and efficiency.

III. DTN ARCHITECTURE

In this research section, we suggest a secure scheme of data retrieval based on attribute set using CP-ABE for DTN's which are decentralized. The suggested scheme attributes achieve an immediate revocation by enhancing forward/backward secrecy of private data by reducing vulnerability windows. Next, encryptors in CP-ABE can define an analytical access policy issued under attributes and any select pair of authorities. Finally, the problem of key escrow is resolved by issuing an escrow-free protocol which exploits decentralized DTN architecture characteristics. The protocol to issue key can generate and issue a secret key to the user by a protocol called 2PC abbreviated as two party computations among the key authorities based on their own underlying secrets.

The 2PC protocol discourages the key authorities in obtaining any confidential information among each other so that no user alone can generate an entire set of user keys. So it is not needed to the user to trust fully the authorities and to protect their confidential shared data among. The confidentiality and the privacy of the data can be enforced cryptographically in opposition to any interested key authorities in the suggested scheme. The paper described an architecture depicted with security model in figure1 as follows:

1. *Key Authorities:* A group of people is a key generation centers generate public or secret CP-ABE parameters. The centralized area consists of key authorities establishes more reliable and secure communication network among a key central authority and every local authority at the time of key setup and phase generation. Every internal authority will manage non-identical attributes and corresponding key attributes are issued to the user. They also grant access privileges to each used based on their attributes. At any case the key authorities will never get compromised and always maintains confidentiality.

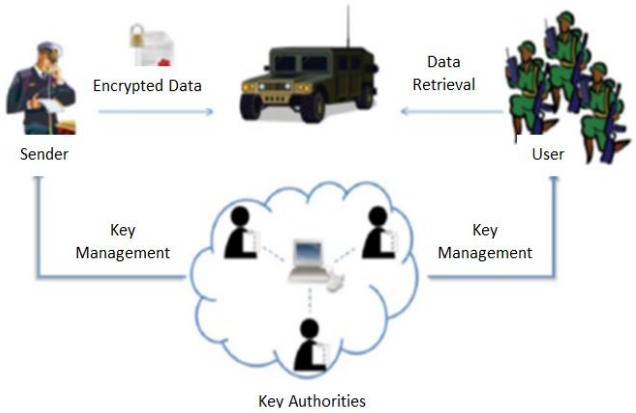

Figure 1: Architecture representing Secure Data Retrieval in DTN's

Figure 1 shows the DTN architecture which consists of the system entities such as

2. *Storage node:* It is an entity which stores data received from sender and provides access to users and it may be static and similar to the existing schemes.

3. *Sender:* A person or an entity that owns confidential data and interested to store the same into the external storage node for better sharing and reliable delivery among the users in the extreme communication environment. The sender is sole responsible to define attribute-based access policy and to apply on its personal data by converting into cipher text before storing it in the node.

4. *User:* A person or a mobile node entity who need to access the stored data at the storage node end. If a user has a pair of attributes obeying the policy of access for the cipher text defined by the entity sender, and then will be to retrieve the encrypted text and obtain the original plain text.

As the key authorities play semi-trusted role, they should be discouraged in accessing plaintext from the storage node. Simultaneously still they can be able to provide secret key to an individual user. To provide the key the local authorities involve in the utilization of 2PC protocol issued independent of key components at the time of issuing key to the user. 2PC protocol is very efficient in not making anyone to generate an entire set of secret keys of the individual user. This is implemented efficiently because the central key authorities never involve in guessing the pair of secret keys of an individual user.

In the area of data analysis and security, we analyze first and compare the efficiency of the suggested scheme to the

current CP-ABE schemes in an aspect of theory. Then, its efficiency is revealed in the simulation network in terms of communication cost. We studied its efficiency while implementing with a pair of specific parameters and to compare the results obtained by the other schemes. Later the paper also analyzed the security requirements in terms of collusion resistance, data confidentiality, backward and forward secrecy.

IV. Simulation

In the DTN application simulation, we considered attribute based encryption using the protected internet. Anmar and Almeroth demonstrated a group behavior and showed that user joining a group will follow a rate with Poisson distribution, and the duration time of the membership following an exponential sharing with a 1/μ mean duration.

We considered that user identically and independently can join and exit events distributed in each group of attributes followed by Poisson distribution. The duration time of membership for an attribute is supposed an exponential distribution following. We also set the time of interarrival among users as 20 minutes with an average duration time of membership as 20 h. Fig. 2 represents the count of current and revoked users in a multiple attribute during the time100 h.

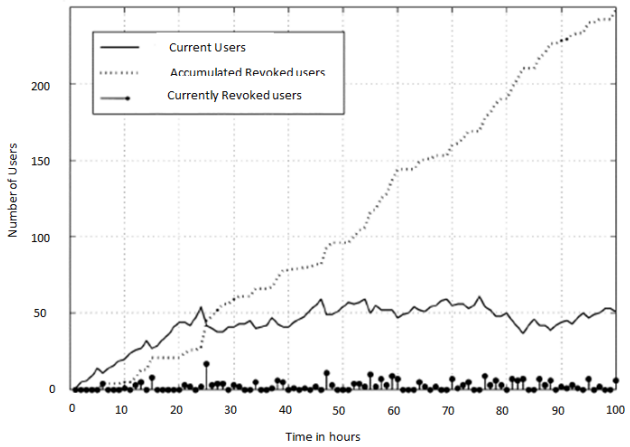

Figure 2: Graph representing the measure of cost computation

Finally, we analyzed and measure the cost of computation by a sender for encrypting and by a user decrypting a data. We therefore observed that there is a balance among computational overhead and access control granularity, which is related closely to the mean of vulnerability. However, the cost of computation by a sender for encryption and by a user for decryption more efficient when compared with other multi-authority schemes.

V. Conclusion

DTN application technologies are the best successful solutions in military environments. They allow secure channel for the wireless devices to communicate among them to exchange the more confidential data reliably. CP-ABE is a mechanism which can solve the problem of inherent key escrow by providing a confidential and guarantee secure data retrieval even though the multiple authorities are not trusted fully or compromised.

Acknowledgment

I want to take this opportunity to thank all the people especially my guide B.V.S.P Pawan Kumar who helped me during my journal sojourn. I understand that it is rather late to acknowledge their contributions, but as the saying goes, better late than never!

References

[1] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp.1–6.

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

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

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

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

[7] 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.

[8] 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.

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

[10] 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.

[11] S. Rafaeli and D. Hutchison, "A survey of key management for secure group communication," *Computing Survey*, vol. 35, no. 3, pp. 309–329, 2003.