Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Secure Data Retrieval For Decentralized Disrutption Tolerant Networks

Shubha N S [1], Swathi N S [2], Swathi G S [3], Rishi Sharma [4] , Rajesh N [5]
[1,2,3,4,5] *Department of Information Science and Engineering, NIE Mysore*

Abstract—Mobile nodes in military network scenarios carried by soldiers may be temporarily disconnected due to jamming and environmental factors. Disruption-tolerant network (DTN) technologies provide storage nodes to store the messages when there is no end-to-end connection. Attribute-based-encryption (ABE) is an approach that enables an access control over encrypted data using access policies and attributes, but this introduces several security and privacy challenges. Here we propose a secure data retrieval scheme using Cipher-text-policy ABE for decentralized DTNs that provides a scalable way of encrypting data. The proposed scheme features immediate attribute revocation, provides fine-grained access policy and resolves key escrow problem.
Keywords— CP-ABE, DTN, Key-Escrow, Access Policy**,** Attribute.

I.INTRODUCTION

In military environments, mobile nodes may be temporarily disconnected due to various environmental factors, jamming and mobility. Disruption-tolerant network (DTN) technologies allow an intermediate node for communication when there is no end-to-end connection between the two nodes [1]-[3].

Military applications require more protection for confidential data which is provided using access control policies. This allows only an authorized person to access the data. Access policies can be provided based on attributes of the user. Key authorities manage these attributes.

Storage nodes in DTN's were introduced to store the data, when there is no end-to-end connection between the source node and the destination node [4], [5]. In DTN technology multiple authorities manage their attribute keys independently.

Attribute-based encryption (ABE) is an approach which provides access control over encrypted data using access policies and attributes [6], [7]. Key authorities produce public and private keys. Users need to possess attributes and private keys to access the encrypted data.

The problem of ABE is that it introduces security challenges. A user might compromise keys or immediate updation of attribute keys may not take place. This becomes an issue in ABE and is more difficult to apply this for multiple users who share the attributes.

In Cipher text policy attribute-based encryption (CP-ABE) method key authorities generate keys for users where a single trusted authority has power to generate whole key. Thus, key authority can decrypt the cipher text. When the multiple authorities manage attribute keys independently it is hard to define fine grained access policy.

A. Existing System

In the concept of ABE system encryption and decryption are determined by the attributes of data. It allows the users to access the encrypted data using access policies and attributes.ABE system enables the use of multiple attributes simultaneously.

B. Disadvantages of Existing System

An important issue with ABE method is that a single authorized person generates the key for the users. Thus the key authorities access the message by decrypting the cipher text.

Another challenge is when multiple key authorities generate keys to users independently; it is difficult to define fine grained access policy.

The problem with ABE method is that immediate key revocation does not takes place. User may change these attributes or they might compromise with keys. In such a situation it is necessary for immediate key updation. This problem is much more difficult for multiple users who share the attribute.

C. Related Work

Max Prop Routing for Vehicle-Based Disruption-Tolerant Networks: DTN's provide intermediate nodes to route network messages. Routing in such environments is difficult because peers have little information about the state of the partitioned network and transfer opportunities between peers are of limited duration.

In Max Prop, a protocol for effective routing of DTN messages is introduced. Max Prop prioritizes the schedule of packets transmitted to other peers and also the schedule of packets to be dropped. These priorities are decided based on the path likelihoods to peers according to collected statistics and also on several complementary mechanisms, including acknowledgments and a head-start for new packets.

Evaluations show that Max Prop performs better than other protocols. Evaluations are based on the real DTN network which has been deployed. It also evaluates Max Prop on simulated topologies and show that it performs well in a wide variety of DTN environments.

Message Ferry Route Design for Sparse Ad Hoc Networks with Mobile Nodes: Message ferrying is a networking model where a special node, called message ferry is used. It facilitates the connectivity in a mobile ad hoc network where the nodes are sparingly deployed. One of the key challenges under this pattern is that, to design the ferry routes to achieve certain properties of end to-end connectivity, such as, delay and message loss among the nodes in the ad hoc network.

This is much more difficult when the nodes in the network move randomly. As we cannot be assured of the location of the nodes, we cannot design a route where the ferry can contact the nodes with confidence. Due to this difficulty, prior work has either considered ferry route design for ad hoc networks where the nodes are inactive, or where the nodes and the ferry move pro-actively in order to meet at certain locations. Such systems either require long-range radio or disrupt nodes' mobility models which can be dictated by non-communication tasks.

A message ferry route is an algorithm that is called as Optimized Way-points (OPWP). It generates a ferry route which assures good performance without requiring any online collaboration between the nodes and the ferry. The OPWP ferry route comprises a set of way-points and waiting times at these way-points. These points are chosen carefully based on the node mobility model. Each time that the ferry traverses this route, it contacts each mobile node with a certain minimum possibility.

The node-ferry contact probability is determined by the frequency of node-ferry contacts and the properties of end-to-end delay. An OPWP consistently performs well.

D. Proposed System

We propose a scalable way of encrypting data using CP-ABE. In which attributes defined by encryptor must be possessed by the decryptor to decrypt the cipher text. In this method, authorized users who have enough credentials can only access the data in the storage node. Thus it increases the protection for confidential of data.

When multiple users combine their attributes they may be able to decrypt the cipher text. CP-ABE method provides fine grained access policy. Thus, it resists the collision [6], [7]. Multiple key authorities generate the key by Two-party computation (2PC) protocol among the key authorities. Thus, it avoids the key authorities from obtaining master secret information.

II.NETWORK ARCHITECTURE

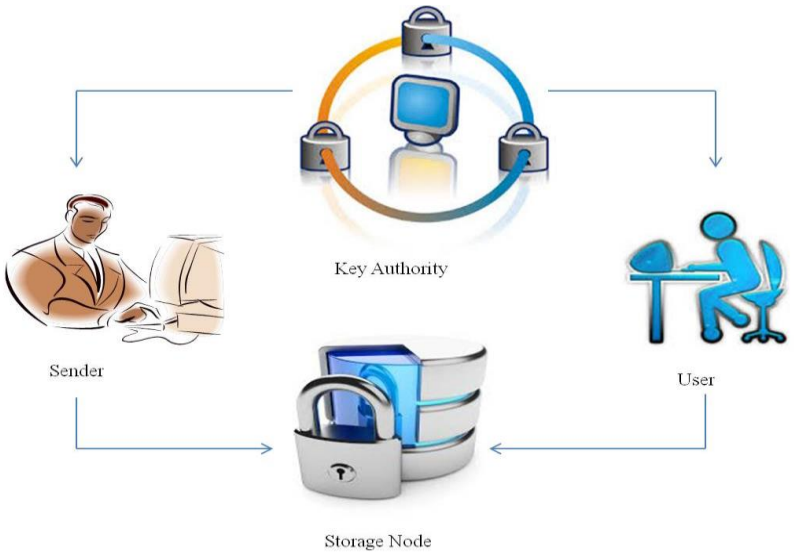

Fig. 1 Architecture of secure data retrieval for DTN's

A. Modules

*Fig.*1 shows the architecture of secure data retrieval for DTN. As shown in the Fig.1 architecture consists of following entities.

- Sender: This is an entity who owns message or data. He sends data to users which are stored in storage node when there is no intermittent connection between sender and user. Sender defines policies and also encrypts data under that policy.

- User: This is an entity who wants to access the data in the storage node. To view the message user has to decrypt the cipher text by possessing attributes. When these attribute satisfy access policy only then the user can obtain the data.

- Key authority: They generate keys for sender and user. There is central authority and many local authorities. They communicate with each other and produce secret key for users.

- Storage node: This entity store data sent from sender and allows authorized users to access the data. It stores an encrypted data from sender. Users can decrypt this data by possessing access policy.

III.ADVANTAGES OF PROPOSED SYSTEM

It provides immediate attribute revocation reduces the windows vulnerability. It enhances forward and backward secrecy of private data.

Forward secrecy means that any user who leaves the attribute must be prevented from accessing the data after he drops the attribute. Backward secrecy means that any new user who enters the attribute must be prevented from accessing the data sent before he enters that attribute.

Multiple key authorities generate keys by communicating with each other. Thus, none of the authorities can alone generate whole set of user's key. Hence it resolves key escrow problem [6].

Multiple key authorities manage the attributes and keys for users and they can define a fine grained access policy over these attributes.

IV.CONCLUSION

DTN technologies in military networks allow devices to communicate with each other using storage node. CP-ABE provides scalable way of solution. In this paper, we propose ABE secure data retrieval scheme using CP-ABE for decentralized DTN. It provides immediate attribute key revocation, enhances forward and backward secrecy of private data.

Multiple authorities manage the attributes and generate keys by communicating with each other. Key escrow problem is resolved maintaining security and privacy of data. In addition, fine grained access policies are provided.

REFERENCES

[1] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in *Proc.IEEE INFOCOM*, pp. 1–11, 2006.
[2] M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, pp. 1–6, 2006.
[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*, pp. 37–48, 2006.
[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*, pp. 1–7, 2007.
[6]A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, pp. 457–473, 2005.
[7] 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*, pp. 89–98, 2006.

