Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.198 – 201

SURVEY ARTICLE

A Survey on Fault Tolerant Data Retrieval in Military Network

Naveen K B[1]
Student, M.Tech (Computer Networking Engineering), BITM, Bellary, India[1]

Pratibha Mishra[2]
Assistant Professor, Computer Science & Engineering Department, BITM, Bellary, India[2]
naveenkb292@gmail.com, iet_pratibha@yahoo.com

Abstract- In military environments, like battlefield or a hostile region, the mobile nodes might suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technology is the successful solution that allow, wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Here, authorization policies are needed in order to retrieve the data securely. Ciphertext-policy attribute-based encryption (CP-ABE) can be provided as the cryptographic solution for the control issues. CP-ABE is applied to the decentralized DTNs. It introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. Here, a scheme where decentralized DTNs use's CP-ABE with multiple key authorities to manage their attributes with mutual communication is used.

Key terms: DTN, Attribute Revocation, Key Escrow, ABE, CP-ABE.

I. INTRODUCTION

In many applications in which the data has to be transmitted over a network where an end-to-end path between source and destination does not exist i.e. in wireless network, the data or the message has to be secured from the unauthorized users. An [2] end-to-end path between a source and a destination pair may not always exist where the links between intermediate nodes may be opportunistic, predictably connectable, or periodically connected. To allow the nodes to communicate with each other in these extreme networking environments, the research community has proposed a new architecture called the disruption tolerant network (DTN). Several DTN routing schemes have been proposed. Typically, the source node's message may need to wait in the intermediate nodes for substantial amount of time when there is no connection to the final destination. After the connection is eventually established, the message is delivered to the destination node.

Disruption-tolerant network (DTN) technologies are the successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Three categories [7] of forwarding schemes have been proposed for DTNs. In the first category is to use message ferries to gather data from stationary sources and deliver them to their destinations. For example, assume that traffic demand between two nodes can be estimated. Then, they design routes for multiple ferries that can minimize the average data delivery latency. They also consider how nodes can be assigned to ferries based on different assumptions about ferry interactions. In the second category, using history-based routing where each node maintains a utility value for every other node in the network, based on a timer indicating the time elapsed since the two nodes last encountered each other. These utility values which carry indirect information about relative node locations, get diffused through nodes' mobility. In the third category, using a 2-hop relay forwarding scheme where the source sends multiple copies to different relaying nodes and the relaying nodes will deliver the copies they have to the destination node when they encounter the destination node.

Ciphertext-Policy Attribute Based Encryption (CP-ABE) is a promising cryptographic primitive for the access control of shared data. In CP-ABE, each user is associated with a set of attributes and data is encrypted with access structures on attributes. A user is able to decrypt a ciphertext if and only if his attributes satisfy the ciphertext access structure. Beside this basic property, practical applications usually have other requirements [5]. Here the challenge [1] is the key escrow problem. 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. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys. 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. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute- based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem.

II. Literature Review

Attribute Based Encryption:

Sahai and Waters first introduced attribute based encryption (ABE) [5] for encrypted access control. The ABE systems can be viewed as a generalization of Identity Based Encryption (IBE) systems [2]. In IBE systems, only one attribute is used which is the identity of the receiver, whereas ABE systems enable the use of multiple attributes simultaneously. In an attribute-based encryption [4] system ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext if there is a "match" between his private key and the ciphertext.

ABE comes in two flavors [1] 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. However, the roles of the ciphertexts and keys are reversed in CP-ABE. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. A sender encrypts [9] a message with an access control policy tree which is logically composed of attributes. Receivers are able to decrypt the message when their attributes satisfy the policy tree. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors such as a commander to choose an access policy on attributes and to encrypt confidential data under the access structure via encrypting with the corresponding public keys or attributes.

Attribute Revocation:

One issue here is attribute revocation [5]. The key revocation problem can be solved by extending each user attribute with an expiration date. It requires the users to periodically go to the authority for key reissuing and thus is inefficient. Enhancement to this solution is provided by associating the user secret key with a single expiration date. This solution places a lower load on the authority as users need to update their keys less frequently. However, this method is not able to realize user attribute change in a timely fashion. These solutions can just disable a user secret key at a designated time, but are not able to revoke a user attribute/key on the ad hoc basis. Boldyreva et al. proposed an efficient revocation scheme for IBE, and the proposed scheme is also applicable to KP-ABE and fuzzy IBE. However, its applicability to CP-ABE is not clear.

Key Escrow:

Most of the existing ABE schemes are constructed on the architecture where a single trusted authority has the power to generate the whole private keys of users with its master secret information. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time. Chase *et al.* presented a distributed KP-ABE scheme that solves the key escrow problem in a multi-authority system. In this approach, all attribute authorities are participating in the key generation protocol in a distributed way such that they cannot pool their data and link multiple attribute sets belonging to the same user [1].

Multi-Authority Attribute-Based Encryption:

A new multi-authority Attribute-Based Encryption system [6] where any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an authority by creating a public key and issuing private keys to different users that reflect their attributes. Different authorities need not even be aware of each other. The concept is of using global identifiers to “link" private keys together that were issued to the same user by different authorities. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Here each authority is responsible for different attributes [8], they are supposed to issue decryption keys independently, without having to communicate with one another. In order to prevent collusion in such a setting, some consistent notion of identity is needed. The solution is to require that each user have a unique global identifier (GID), which they must present to each authority.

Decentralized system:

Decentralized system [6] does not require any central authority. Thus, the performance bottleneck incurred by relying on a central authority can be avoided, which makes the system more scalable. Also avoid placing absolute trust in a single designated entity which must remain active and uncorrupted throughout the lifetime of the system. This is a crucial improvement for efficiency as well as security, since even a central authority that remains uncorrupted may occasionally fail for some reasons, and a system that constantly relies on its participation will be forced to remain stagnant until it can be restored. Here, authorities can function entirely independent, and the failure or corruption of some authorities will not affect the operation of functioning, uncorrupted authorities. This makes decentralized system more robust than the other approaches. One disadvantage [1] of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key. This results in communication overhead on the system setup and the rekeying phases and requires each user to store additional auxiliary key components besides the attributes keys, where is the number of authorities in the system

III.CONCLUSION

The secure and efficient data retrieval will be provided while communicating through the wireless devices, in order to communicate with each other and access the confidential information reliably by exploiting external storage nodes. And the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted.

REFERENCES

[1] Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM, 2014.

[2] 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.

[3] 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.

[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption," in Proc. IEEE Symp. Security Privacy, 2007, pp. 321–334.

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

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

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

[8] M. Chase and S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

[9] 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.