ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CP-ABE mechanism for managing confidential data efficiently in Disruption Tolerant Networks

N. Tejashwini
MTech Student,
Department of CSE,
SreeVisvesvaraya Institute Of Technology & Science,
MahabubNagar,Telangana,India.

N.VenkateshNaik,
Research scholar,
Department of CSE,
Jawaharlal Nehru Technological University- Anantapur, (JNTUA)
A.P.,India.

DrK.Madhavi
Assistant Professor
Department of CSE,
Jawaharlal Nehru Technological University- Anantapur, (JNTUA)
A.P.,India.

Abstract: ***Disruption-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise. In the current paper we take the example of Military networks. The concept of attribute-based encryption (ABE) is a promising approach that full fills the requirements for secure data retrieval in DTN.In this paper, we implement a safe information recovery plan utilizing CP-ABE for decentralized DTNs where numerous keypowers deal with their qualities autonomously. We show how to apply the proposed mechanism to safely and proficiently deal with the classified information dispersed in the Disruption Tolerant Networks.***

Keywords:*Attribute-based encryption (ABE), Disruption-tolerant network (DTN), Secure-data retrieval, Session management, Bundle protocol, Access control.*

Introduction:

The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Delay and disruption-tolerant networks (DTNs), are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. In these challenging environments, popular ad hoc routing protocols such as AODV and DSR fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data. However, when instantaneous end-to-end paths are difficult or impossible to establish, routing protocols must take to a "store and forward" approach, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination. A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination. This is feasible only on networks with large amounts of local storage and internode bandwidth relative to the expected traffic. In many common problem spaces, this inefficiency is outweighed by the increased efficiency and shortened delivery times made possible by taking maximum advantage of available unscheduled forwarding opportunities. In others, where available storage and internode throughput opportunities are more tightly constrained, a more discriminate algorithm is required.

Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity because the network hinders complicated cryptographic protocols, hinders key exchange, and each device must identify other intermittently visible devices. Solutions have typically been modified from mobile ad hoc network

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

and distributed security research, such as the use of distributed certificate authorities and PKI schemes. Original solutions from the delay-tolerant research community include: 1) the use of identity-based encryption, which allows nodes to receive information encrypted with their public identifier; and 2) the use of tamper-evident tables with a gossiping protocol.

Related Work

In CP-ABE, is taken for the encryption policy and in the transferred data is taken to this step but a key is simply created with respect to an attributes set. CPABE is more appropriate to DTNs than KP-ABE because it enables encryptions 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 ABE comes in two flavors called key-policy ABE (KP-ABE) and cipher text-policy ABE(CPABE).In KP-ABE, the encrypted only gets to label a cipher text with a set of attributes. The each user is having the different policy from the key authority that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user's key.

1) Key Escrow

The secret information that are encrypted for the key of the single master and he is the one is having the all the power and the master can view the key when generating Thus the key escrow problem is following such that the key authority can decrypt every cipher text addressed to users in the same group generating their secret keys at any time.

2) Attribute Revocation

Key evocation mechanisms in CP-ABE and KP-ABE, respectively. The solutions are to relate to each attribute expiration the date or time and distribute a new set of the keys to real users after that it expiration. The periodic attribute revocable schemes have two main problems. The first and fore most problem is the security issue in terms of the Back ward and forward secrecy. It is a considerable scenario that users such as soldiers may change their attributes frequently, e.g., position or location move when considering that.

3) Revocation

The keys of a user without rekeying the whole set of key components of the user in ABE key structure since the whole key set of a user is bound with the same random value in order to prevent any collusion attack. Therefore, revoking a single attribute in the system requires all users who share the attribute to update all their key components even if the other attributes of them are still valid. This seems very inefficient and may cause severe overhead in terms of the computation and communication cost, especially in large-scaled DTNs Shows the authority architecture, logic expressiveness of access structure that can be defined under different dis joint sets of attributes managed by different authorities, key escrow, and revocation granularity of each CP-ABE scheme. In the previous scheme the logic can be very expressive that the same BSW single authority such that the access policy can be expressed with any monotone access structure under attributes of any chosen set of authorities; while HV the schemes only allow the AND gate among the sets of attributes managed by different authorities. The revocation in the proposed scheme can be done as to the BSW in the immediate way it taken. Therefore, the user of the attribute is revokes that at any time even before the expiration time.

4) Efficiency of encryption

In addition, the proposed scheme realizes more fine-grained user revocation for each at- tribute rather than for the whole system as opposed to RC. Thus, even if a user comes to hold or drop any attribute during the service in the proposed scheme, he can still access the data with other attributes that he is holding as long as they satisfy the access policy defined in the cipher text. The key escrow problem is also resolved in the proposed scheme such that the confidential data would not be revealed to any curious key authorities. Table summarizes the efficiency comparison results among CP-ABE Schemes. As shown in Table the proposed

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

scheme needs rekeying message size of at most to realize user-level access control for each attribute in the system. Although RC does not need to send additional rekeying message for user revocations as opposed to the other schemes, its cipher text size is linear to the number of revoked users in the system since the user revocation message is included in the cipher text. The proposed scheme requires a user to store more KEKs.

5). Key Updating

If the single key is used we can't be to secure more we need the key updating the same algorithm and a new algorithm is used for the updating of the key and it is mandatory.

Existing System:

The concept of attribute-based encryption (ABE) is a promising approach that fulfills the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.

Disadvantages Of Existing System:

1. The problem of applying the ABE to DTNs introduces several security and privacy challenges. Since some users may change their associated attributes at some point (for example, moving their region), or some private keys might be compromised, key revocation (or update) for each attribute is necessary in order to make systems secure.

2. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, we refer to such a collection of users as an attribute group)

3. Another challenge 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.

4. The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities.

Proposed System:

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

Advantages Of Proposed System:

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. In addition, unauthorized access

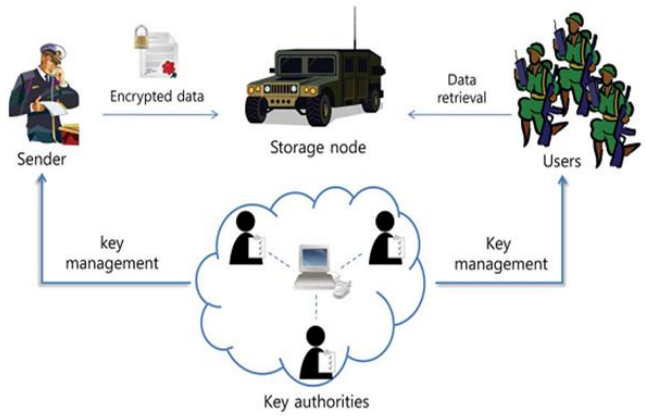
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

from the storage node or key authorities should be also prevented.

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.

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 previous 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 subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

System Architecture:



Modules:

1. Key Authorities
2. Storage Nodes
3. Sender
4. User

Modules Description:

Key Authorities:

They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each 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 assumed 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 encrypted contents as much as possible.

Storage node:

This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semi-trusted that is honest-but-curious.

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.

User:

This is a mobile node who wants to access the data stored at 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.

Conclusion

In military area the DTN technology is now booming because the network is secure and efficient and in which the session management is used to reduce the traffic and the new bundle protocol is used for the efficiency of the network the DTN technology is used

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

because as it is the military environment signal is may or may not be in which we are having the collusion loss and to overcome that we are using the technology and in which previous the store and forward technique is used and in which less packet that be transmitted and the it is less efficient, to overcome that bundle protocol is used and it booming now a days and it is using in the space and the for the disaster management in which the routers is used to transmit the signals for the security CP-ABE technique is used.

References:

[1] JunbeomHur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks"-IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 22, NO. 1, FEBRUARY 2014.

[2]M. Ramesh Reddy &S.Vasu, Distributed Detection Of Node Replication Attacks In Disruption Tolerant Networks, IJMETMR (http://www.ijmetmr.com/olseptember2014/RameshReddy-SVasu-16.pdf), Volume No: 1(2014), Issue No: 9 (September)

[3] J.Burgess, B.Gallagher, D.Jensen, and B.N.Levine, "Maxprop:Routing for vehicle-based disruption tolerant networks," in Proc.IEEE INFOCOM, 2006,

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

[5] M.M.B.Tariq, M.Ammar, and E.Zequra, "Mesage ferry route design for sparse ad hoc networks with mobile nodes," in Proc. ACM Mobic, 2006

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

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

[8] 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

[9] L.Ibraimi,M.Petkovic,S.Nikova,P.Hartel, and W.Jonker, "Mediated cipher text-policy attribute-based encryption and its application in Proc. WISA, 2009, LNCS 5932

[10] N.Chen, M.Gerla, D.Huang, and X.Hong,"Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption,"inProc. Ad Hoc Network. Workshop, 2010

[11] D.Huang and M.Verma, "ASPE: Attribute-based secure policy enforcement in vehicular ad hoc networks," Ad Hoc Network., vol. 7, no. 8,2009.

[12] A. Lewko and B. Waters, "Decentralizing attributebased encryption", Cryptology ePrint Archive: Rep. 2010/351, 2010.

Authors:

N.Tejashwini

N.VenkateshNaik