PROTECT KNOWLEDGE RETRIEVAL FOR DECENTRALIZED DISRUPTION_TOLERANT MILITARY NETWORKS

N. THIRUPATHAMMA[1], K. VENKATESWARA RAO[2]

[1]M-Tech Dept. of CSE SreeVahini Institute of Science and Technology Tiruvuru Andhra Pradesh

[2]Asst.Professor Dept. of CSE SreeVahini Institute of Science and Technology Tiruvuru Andhra Pradesh

Abstract:

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming 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. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper, we propose a secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Keywords: *Access control, attributes based encryption (ABE), disruption-tolerant networks (DTN), and secures data retrieval*

1. INTRODUCTION

Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles, which are managed by the key authorities. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2." In this case, it is a reasonable assumption that multiple key authorities are likely to manage their own dynamic attributes for soldiers in their deployed regions or echelons, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) . We refer to this DTN architecture where multiple authorities issue and manage their own attribute keys independently as a decentralized DTN.

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 cipher texts. Especially, cipher text-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. However, 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. 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). This implies that revocation of any attribute or any single user in an

Attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other Members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability if the previous Attribute key is not updated immediately.

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. Thus, the key authority can decrypt every cipher text 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.

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. For example, suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B.

Then, it is impossible to generate an access policy (("role 1" OR "role 2") AND ("region 1" or "region2")) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented. This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

2. Related Work

a. Attribute Revocation:

Solutions proposed to append to each attribute an expiration date or time and distribute a new set of keys to valid users after the expiration.

b. 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.

A distributed KP-ABE scheme proposed solves the key escrow problem in a multiauthority system. In this approach, all (disjoint) 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.

c. Decentralized ABE:

A combined access policy over the attributes issued from different authorities by simply encrypting data multiple times. The main disadvantages of this

approach are efficiency and expressiveness of access policy.

3. LITERATURE SURVEY

3.1 Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data:

As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). We develop a new cryptosystem for ¯ne-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our cryptosystem, ciphertext are labeled with sets of attributes and private keys are associated with access structures that control which ciphertext a user is able to decrypt. We demonstrate the applicability of our construction to sharing of audit-log information and broadcast encryption. Our construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

3.2. Decentralizing Attribute-Based Encryption:

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, 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 ABE authority by creating a public key and issuing private keys to different users that react their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority \tied" together different components (representing different attributes) of a user's private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge ciphertext and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of Composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.

3.3 Identity-based Encryption with Efficient Revocation:

Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). Any setting, PKI- or identity-based, must provide a means to revoke users from the system. Efficient revocation is a well-studied problem in the traditional PKI setting. However in the setting of IBE, there has been little work on studying the revocation mechanisms. The most practical solution requires the senders to also use time periods when encrypting, and all the receivers (regardless of whether their keys have been compromised or not) to update their private keys regularly by contacting the trusted authority.

We note that this solution does not scale well – as the number of users increases, the work on key updates becomes a bottleneck. We propose an IBE scheme that significantly improves key-update efficiency on the side of the trusted party (from linear to logarithmic in the number of users), while staying efficient for the users. Our scheme builds on the ideas of the Fuzzy IBE primitive and binary tree data structure, and is provably secure.

3.4 Message Ferry Route Design for Sparse Ad hoc Networks with Mobile Nodes:

Message ferrying is a networking paradigm where a special node, called a message ferry, facilitates the connectivity in a mobile ad hoc network where the nodes are sparsely deployed. One of the key challenges under this paradigm is the design of 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 a difficult problem when the nodes in the network move arbitrarily. As we cannot be certain of the location of the nodes, we cannot design a route where the ferry can con act the nodes with certainty. Due to this difficulty, prior work has either considered ferry route design for ad hoc networks where the nodes are stationary, 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 patterns which can be dictated by non-communication tasks. We present a message ferry route design algorithm that we call the Optimized Way-points, or OPWP, that 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, that 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 probability.

The node-ferry contact probability in turn determines the frequency of node-ferry contacts and the properties of end-to-end delay. We show that OPWP consistently outperforms other naive ferry routing approaches.

3.5 Performance Evaluations of Data-Centric Information Retrieval Schemes for DTNs:

Mobile nodes in some challenging network scenarios, e.g. battlefield and disaster recovery scenarios, suffer from intermittent connectivity and frequent partitions. Disruption Tolerant Network (DTN) technologies are designed to enable communications in such environments. Several DTN routing schemes have been proposed. However, not much work has been done on designing schemes that provide efficient information access in such challenging network scenarios. In this paper, we explore how a content-based information retrieval system can be designed for DTNs. There are three important design issues, namely (a) how data should be replicated and stored at multiple nodes, (b) how a query is disseminated in sparsely connected networks, (c) how a query response is routed back to the issuing node. We first describe how to select nodes for storing the replicated copies of data items. We consider the random and the intelligent caching schemes. In the random caching scheme, nodes that are encountered first by a data-generating node are selected to cache the extra copies while in the intelligent caching scheme, nodes that can potentially meet more nodes, e.g. faster nodes, are selected to cache the extra data copies. The number of replicated data copies K can be the same for all data items or varied depending on the access frequencies of the data items. In this work, we consider fixed, proportional and square-root replication schemes. Then, we describe two query dissemination schemes: (a) W-copy Selective Query Spraying (WSS) scheme, (b) L hop Neighbourhood Spraying (LNS) scheme. In the WSS scheme, nodes that can move faster are selected to cache the queries while in the LNS scheme, nodes that are within L-hops of a querying node will cache the queries. For message routing, we use an enhanced Prophet scheme where a next-hop node is selected only if its predicted delivery probability to the destination is higher than a certain threshold. We conduct extensive simulation studies to evaluate different combinations of the replication and query dissemination algorithms. Our results reveal that the scheme that performs the best is the one that uses the WSS scheme combined with binary spread of replicated data copies.

The WSS scheme can achieve a higher query success ratio when compared to a scheme that does not use any data and query replication. Furthermore, the square-root and proportional replication schemes

provide higher query success ratio than the fixed copy approach with varying node density. In addition, the intelligent caching approach can further improve the query success ratio by 5.3% to 15.8% with varying node density. Our results using different mobility models reveal that the query success ratio degrades at most 7.3% when the community-based model is used compared to the Random Waypoint (RWP) model. Compared to the RWP and the community-based mobility models, the UmassBusNet model from the Diesel Net project achieves much lower query success ratio because of the longer inter-node encounter time.

4. Problem Definition

The problem of applying the ABE to DTNs introduces several security and privacy challenges. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group. For example, if a user joins or leaves an attribute group, the associated attribute key should be changed and redistributed to all the other members in the same group for backward or forward secrecy. It may result in bottleneck during rekeying procedure or security degradation due to the windows of vulnerability if the previous attribute key is not updated immediately.

5. Proposed System:

Especially, cipher text-policy ABE (CP-ABE) provides a scalable way of encrypting data x such that the encryptor defines the attribute set that the decrypted needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. 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.

- To propose attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs.
- 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.
- 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.

5.1 Advantages of proposed systems:

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

- **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 plain text of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

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, encryptor 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.

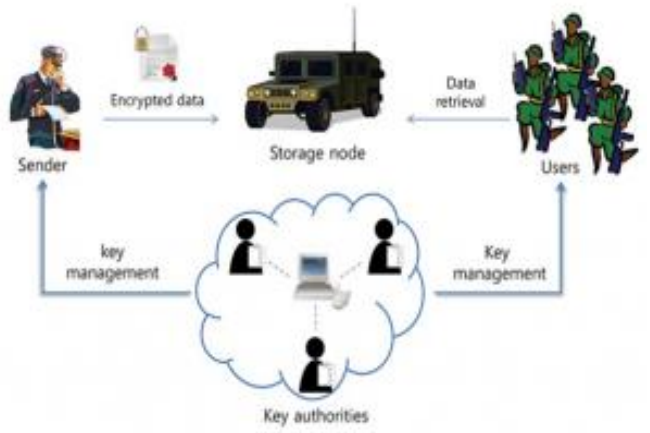

Figure1: The Architecture of Protect knowledge Retrieval for Decentralized Disruption Tolerant Military Networks

6. Modules

1. Key Authorities
2. Storage node.
3. Sender.
4. Soldier (User).
5. CP-ABE Method.

Module Description:

1. 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.

2. 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.

3. 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.

4. Soldier (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.

5. CP-ABE Method:

7. CONCLUSION AND FUTURE WORK

DTN technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE for decentralized

In Ciphertext Policy Attribute based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is sent along with the ciphertext. We propose a method in which the access policy need not be sent along with the ciphertext, by which we are able to preserve the privacy of the encryptor.

This techniques encrypted data can be kept confidential even if the storage server is un trusted; moreover, our methods are secure against collusion attacks. Previous Attribute- Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys;

While in our system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

DTNs where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. In addition, the fine-grained key revocation can be done for each attribute group. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption- tolerant military network.

Acknowledgements

The authors would like to thank the anonymous reviewers for their careful reading and insightful comments that have helped in improving of this paper.

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] 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, 2007, pp. 1–7.

[6] 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.

[7] 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.

[8] 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.

Author Profiles

N.THIRUPATHAMMA
M-Tech Dept. of CSE SreeVahini Institute of Science and Technology Tiruvuru Andhra Pradesh.

K.Venkateswara Rao
Asst.Professor
SreeVahini Institute of Science and Technology
Tiruvuru
Andhra Pradesh " M.Tech "