International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks

Arram Sriram
Asst.Prof, IT Depatment, Anurag Group of Institutions
V: Venkatapur, M: Ghatkesar, D: Rangareddy, Telangana, 501301.
Arram.sriram@gmail.com

Abstract-*Mobile nodes in military environments such as a Battlefield or hostile regions 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, attribute-based encryption (ABE), disruption-tolerant network (DTN),multiauthority, secure data retrieval.*

Introduction

In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments. disruption-tolerant network (dtn) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. roy and chuah introduced storage nodes in dtns where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. Many military applications require increased protection of confidential data including access control methods that are cryptographically enforce.

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.

Node Density-Based Adaptive Routing Scheme for Disruption Tolerant Networks:

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. Hence, routing mechanisms that can withstand disruptions need to be designed. A store-and-forward approach has been proposed for disruption tolerant networks. Recently, several approaches have been proposed for unicast routing in disruption-prone networks e.g. the 2-hop relay approach, delivery probability based routing, and message ferrying. In our earlier paper, we have evaluated a combined multihop and message ferrying approach in disruption tolerant networks.

we assume that a special node is designated to be a message ferry. A more flexible approach is to let regular nodes volunteer to be message ferries when network dynamics mandate the presence of such ferries to ensure communications. Thus, in this paper, we design a nodedensity based adaptive routing (NDBAR) scheme that allows regular nodes to volunteer to be message ferries when there are very few nodes around them to ensure the feasibility of continued communications. Our simulation results indicate that our NDBAR scheme can achieve the highest delivery ratio in very sparse networks that are prone to frequent disruptions. Packet-switched network communication has been studied for decades. Important progress has been made in robustness and scalability in the TCP/IP protocol suite based primarily on principles of end-to-end protocols and services.

Mediated Ciphertext-Policy Attribute-Based Encryption and its Application:
In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the ciphertext is associated with an access policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satis¯es the access policy speci¯ed in the ciphertext. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed. In this paper, we propose a medi- ated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, we demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs). Modern distributed information systems require °exible access control models which go beyond discretionary, mandatory and role-based access control. Recently proposed models, such as attribute-based access control, dene access control policies based on different attributes of the requester, environment, or the data object. On the other hand, the current trend of service-based information systems and storage outsourcing require increased protection of data includ- ing access control methods that are cryptographically enforced.

The concept of Attribute-Based Encryption (ABE) fullls the aforementioned requirements. It provides an elegant way of encrypting data such that the encryptor de¯nes the attribute set that the decryptor needs to posses in order to decrypt the cipher- text. Since Sahai and Waters proposed the basic ABE scheme, several more advanced schemes have been developed, such as most notably Ciphertext-Policy ABE schemes (CP-ABE). In these schemes, a ciphertext is associated with an access policy and the user secret key is associated with a set of attributes. A secret key holder can decrypt the ciphertext if the attributes associated with his secret key satisfy the access policy associated with the ciphertext. For example, consider a situation when two organizations, a Hospital and a University, conduct research in the ¯eld of neurological disorders. The Hospital wants to allow access to their research results to all sta® from the University who have the role Professor and belong to the Department of Neurology (DN). To en- force the policy, the Hospital encrypts the data according to the access policy *¿Results*=(University Professor ^ Member of DN). Only users who have a secret key associated with a set of attributes *!*=(University Professor, Member of DN) can satisfy the access policy *¿Results* and be able to decrypt the ciphertext. The state-of-the-art CP-ABE schemes provide limited support for revocation of attributes, a feature, which is becoming increasingly important in modern access control systems. In general, attribute revocation may happen due to the following reasons: 1) an attribute is not valid because it has expired, for instance, the attribute "project manager-January 2009 " is valid until January 2009, or 2) a user is misusing her secret key associated with a set of attributes, for instance, Alice might give a copy of her secret key to Bob who is not a legitimate user. In particular, attribute revocation is an important requirement in the domain of access control to personal health data, which is our application ¯eld for attribute- based encryption.

Improving Security and Efficiency in Attribute-Based Data Sharing:
With the recent adoption and diffusion of the data sharing paradigm in distributed systems such as online social networks or cloud computing, there have been increasing demands and concerns for distributed data security. One of the most challenging issuesin data sharing systems is the enforcement of access policies and the support of policies updates. Ciphertext policy attribute-based encryption (CP-ABE) is becoming a promising cryptographic solution to this issue. It enables data owners to define their own access policies over user attributes and enforce the policies on the data to be distributed. However, the advantage comes with a major drawback which is known as a key escrow problem.

The key generation center could decrypt any messages addressed to specific users by generating their private keys. This is not suitable for data sharing scenarios where the data owner would like to make their private data only accessible to designated users. In addition, applying CP-ABE in the data sharing system introduces another challenge with regard to the user revocation since the access policies are defined only over the attribute universe. Therefore, in this study, we propose a novel CP-ABE scheme for a data sharing system by exploiting the characteristic of the system architecture.

Performance Evaluation of Content-Based Information Retrieval Schemes for DTNs:
Mobile nodes in some challenging network scenarios suffer from intermittent connectivity and frequent partitions e.g. battlefield and disaster recovery scenarios. Disruption Tolerant Network (DTN) technologies are designed to enable nodes in such environments to communicate with one another. Several DTN routing schemes have been proposed. However, not much work has been done on providing information access in such challenging network scenarios. Existing client/server paradigm for information access will not be feasible in such scenarios since end-to-end path does not exist. Thus, in this paper, we explore how a content-based information retrieval system can be designed for DTNs.

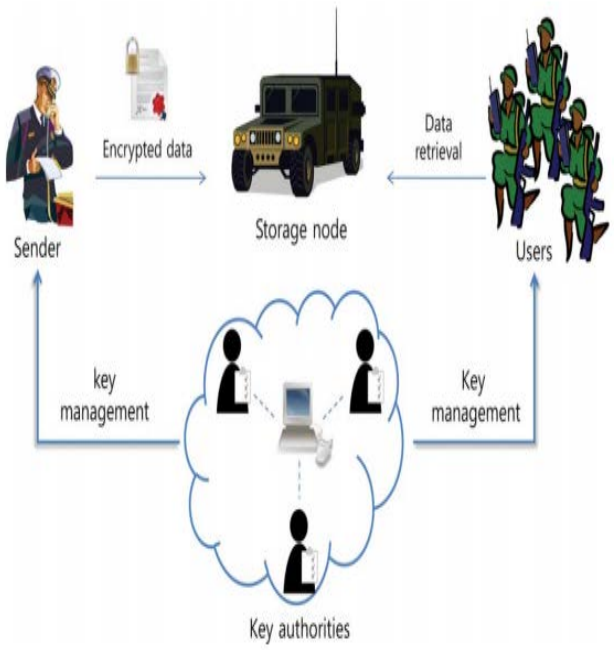
There are three important design issues, namely (a) how should data be replicated and stored at multiple nodes, (b) how should a query be disseminated in sparsely connected networks, (c) how should a query response be routed back to the querying node. We first describe two data caching schemes: (a) K-copy random caching, (b) K-copy intelligent caching. Then, we describe an L-hop Neighborhood Spraying (LNS) scheme for query dissemination. For message routing, we either use Prophet routing scheme or Highest Encounter First Routing (HEFR) scheme. We conduct extensive simulation studies to evaluate different combinations of these

algorithms. Our results reveal that the scheme that performs the best is the one that uses the Kcopy intelligent caching combined with the LNS query dissemination and HEFR scheme. Such adhoc networks are very useful in several scenarios e.g. battlefield operations, vehicular adhoc networks and disaster response scenarios. Many adhoc routing schemes have been designed for adhoc networks but such routing schemes are not useful in some challenging network scenarios where the nodes have intermittent connectivity and suffer frequent partitioning. Several DTN routing schemes have been proposed. Although routing is an important design issue for such sparsely connected networks, the ability to access information rapidly is also an important feature that a DTN should have since the ultimate goal of having such a network is to allow mobile nodes to access information quickly and efficiently.

For example, in a battlefield, soldiers need to access information related to detailed geographical maps, intelligent information about enemy locations, new commands from the general, weather information etc. In addition, a particular data item may be of interests to multiple soldiers so it makes sense to replicate the data item, and store it at multiple nodes so that it can be accessed by other nodes. This allows us to save battery power, bandwidth consumption and the data item retrieval time. Such data caching also means that the source of the data items need not know the identities of the nodes that need to access the data items.

SYSTEM

Architecture



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.

ALGORITHMS

CP-ABE Method :

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 untrusted; 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.

Ciphertext-Policy Attribute-Based Encryption (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.

Public-Key Algorithm: (2pc protocol)

Using of this algorithm Key-Authority can generate Public-Key and Private-Key for Encryption(Ciphertext).

CONCLUSION

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, proposed an efficient and secure data retrieval method using CP-ABE for decentralized 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.

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.

[9] 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.

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