IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE CIPHER TEXT POLICY FOR MILITARY

Shazia Saleem [*], Raafiya Gulmeher

*Department of Computer Science And Engineering, Khaja Banda Nawaz College Of Engineering, India

ABSTRACT

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity. 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. Disruption- tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in this extreme networking environment. The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. 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.

KEYWORDS: - Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

INTRODUCTION

In 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 Disruption-tolerant networks (DTNs) attempt to route network messages via intermittently connected nodes [1]. Routing in DTN environments is difficult as the compeers have some information about the state of the dividing network and transfer opportunities between compeers are of limited time.

In many military applications, requires high 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 specified over attributes of users or roles of users, which are managed and issued by the key authorities. For example, in a disruption-tolerant military network, a major or the sender may store confidential data at a storage node for some amount of time, 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 attributes for soldiers in their deployed regions, which could be frequently changed (e.g., the attribute representing current location of moving soldiers) [1].

The concept of attribute-based encryption (ABE) is a promising approach that fulfils the requirements for secure data retrieval in DTNs. ABE features a mechanism that enables an access control over encrypted data using access policies. 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 [1].

EXISTING SYSTEM

The concept of attribute-based encryption (ABE) is a promising approach that fulfils secure data retrieval in DTNs. ABE has a mechanism that enables an access control over encrypted data using access policies. However, applying the ABE to DTNs introduces several security and privacy challenges [1] with regard to key revocation, key escrow, and coordination of attributes. In case of key revocation, since some users may change their attributes at some time for example, changing their region then in this case updating is important in order to have a secure system. This is difficult in ABE system since single attribute is shared by many users, updating of any attribute in an attribute group would affect the other user in a group who are sharing an attribute. For example, if a user joins or leaves an attribute then the associated attribute key should be changed and redistributed to all other members in the group. This results in hazard during rekeying procedure. In CP-ABE, key authority will develops secret keys of users by applying their master key to the attribute set associated with the users [1]. If key authorities are compromised then it is a threat to confidential data. With regard to coordination of attributes, when multiple authorities issues keys to the users independently by applying their own master key, then it is hard to define the fine-grained access policy. The limitations of this system are firstly, if the key authority is compromised by adversaries when deployed in the hostile region, this could be a potential threat to data confidentiality or privacy especially when data is high sensitive. Secondly, it is very hard to define fine-grained access policies.

PROPOSED SYSTEM

In proposed system a technique was developed that gives more protection to sensitive data that is transferred in military environment this technique is CP-ABE. As the key authority can develop secret keys of users by applying master secret keys to users associated set of attributes, there will be threat to the data as long as the authorities have whole privilege to develop secret keys by applying their own master keys [1]. This is resolved in the proposed system by using an access structure that is monotone under the attributes issued from different authorities. Key escrow problem is also solved using escrow-free key issuing protocol that develops and issues user secret key by performing 2PC protocol that avoids the key authorities to determine the key for a specific user. The advantages of this system are, immediate attribute revocation enhances forward/backward secrecy of confidential data by reducing windows of vulnerability,encryptor can define fine-grained access policies using a monotone access structure under attribute issued from any chosen set of authorities and the key escrow problem is resolved by an escrow-free key issuing protocol.

RELATED WORK

ABE comes in two flavours called key-policy ABE (KP-ABE and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor only labels a ciphertext with a set of attributes. The key authority chooses a policy for each user that determines which ciphertext he can decrypt and issues the key to each user by embedding the policy into the user’s key. In CP-ABE, access policy need to be sent along with the ciphertext. The user will only be able to decrypt the ciphertext if he has the attributes that satisfies the access policy and obtain the message. CP-ABE is more appropriate to DTNs than KP-ABE. Applying CP-ABE to DTNs introduces security and privacy challenges such as attribute revocation, key escrow, and coordination of attributes.

1) *Attribute Revocation*: - Reference [6] shows Attribute revocation as the first key revocation mechanism in KP-ABE and CP-ABE The first problem with this is the security degradation in terms of the backward 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 these as attributes. Then, a user who newly holds the attribute might be able to access the previous data (backward secrecy).On the other hand, a revoked user would still be able to access the encrypted data even if he does not hold the attribute any more (forward secrecy).
The other is the scalability problem. The key authority periodically announces a key update material by unicast at each time-slot so that all of the non-revoked users can update their keys. This results in the “1-affects-n” problem, which means that the update of a single attribute affects the whole non- revoked users who share the attribute.
2) *Key escrow:* - Most of the existing ABE schemes are constructed on the architecture that where a single authority has the power to generate the whole private keys of users with its master secret information as in [5], [6], [8]. Thus the key escrow problem is inherent. KP-ABE scheme solves the key escrow problem in a multi-authority system.
3) *Decentralised ABE*:-Decentralised CP-ABE scheme in multiauthority network environment is proposed in [9]. They achieved the combined access policy over the attributes issued from different authorities.
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 introduced in [1] enables nodes in such environments to communicate with one another. Several application scenarios require a security design that provides fine grain access control to contents stored in storage nodes within a DTN. An access control scheme which is based on the Ciphertext Policy Attributed-Based Encryption (CP-ABE) approach is proposed. A flexible fine-grained access control scheme is provided such that the encrypted contents can only be accessed by authorized users. Two unique features of scheme are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature.

Disruption-tolerant networks (DTNs attempt to route network messages via intermittently connected nodes. 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. Maxprop, a protocol for effective routing of DTN messages is introduced in [2]. Maxprop is based on prioritizing both the schedule of packets transmitted to other peers and the schedule of packets to be dropped.

Routing mechanisms that can withstand disruptions called as store-and-forward approach for delivering messages in disruption tolerant networks is proposed in [3]. 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 schemes. They assumed 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. Several routing schemes have been proposed for DTNs. They can be categorized into three categories: (i) using message ferries to connect partitioned nodes (ii) using history-based information to estimate delivery probability of peers and pass the message to the peer that can best deliver the message and (iii) using 2-hop relay forwarding schemes where a source can send multiple copies to different relay nodes and have the relay nodes deliver to the destination when they encounter the destination.

A content-based information retrieval system for DTN is introduced in [4].Several DTN routing schemes have been proposed. But, not much work has been done on designing schemes that provide efficient information access in such challenging military network scenarios. 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.

An Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of *any* access formula over attributes is described in [5]. Previous ABE schemes were limited to expressing only monotonic access structures. A proof of security is provided for this scheme based on the Decisional Bilinear Diffe-Hellman (BDH) assumption. Furthermore, the performance of this scheme compares favourably with existing, less-expressive schemes.

In distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. If any server storing the data is compromised, then the confidentiality of the data will be compromised. A system for realizing complex access control on encrypted data called as Ciphertext-Policy Attribute-Based Encryption is presented in [6]. By using this technique encrypted data can be kept confidential even if the storage server is untrusted.

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 satisfies the access policy specified in the ciphertext. Several CP-ABE schemes have been proposed, however, some practical problems, such as attribute revocation, still needs to be addressed. A mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) is proposed in [7], which extends CP-ABE with instantaneous attribute revocation.

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). A new cryptosystem for fine-grained sharing of encrypted data called as Key-Policy Attribute-Based Encryption (KP-ABE) is developed [8]. In this cryptosystem, ciphertext are labelled with sets of attributes and private keys are associated with access structures that control which ciphertext a user is able to decrypt.

Multi-Authority Attribute-Based Encryption (ABE) system is introduced [9]. In this 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 create their attributes. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Finally, system does not require any central authority.

Protecting identity in the Internet age requires the ability to go beyond the identification of explicitly identifying information like social security numbers, to also find the broadly held attributes that, when taken together, are identifying. A system is presented in [10] that can work in conjunction with natural language processing algorithms or user-generated tags, to protect identifying attributes in text. The system uses a new attribute-based encryption protocol to control access to such identifying attributes and thus protects identity. The system supports the definition of user access rights based on role or identity.

SYSTEM ARCHITECTURE

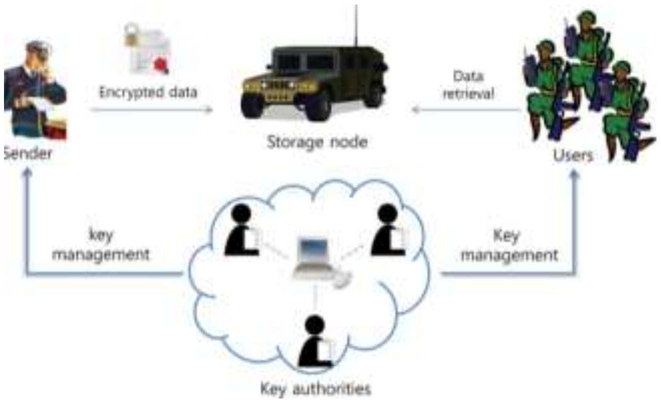

Fig 1.Architrcture of secure data retrieval in a disruption-tolerant military network

The architecture consists of the following system entities.
1) *Key Authorities*: They are key generation centres that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities [1]. The central authority will develop keys to the local authority and local authority in turn will develop keys for the sender and the user. We assume that there are secure a communication channels between a central authority and each local authority during the initial key setup and generation phase [1]. 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 [1].This means that they will honestly execute their work but will be able to acquire the data.
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. As soon as the data is sent to the storage node the will transmit the data in no time.
3) *Sender:* This is an entity that has confidential messages or data (e.g., a commander) and wishes to store them into the storage node for ease of sharing to users in the extreme networking environments. A sender is responsible for defining (attribute-based) access policy and enforcing it on the encrypted data before storing it to the storage node.
4) *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, then he will be able to decrypt the ciphertext and obtain the data.

ALGORITHMS

A ciphertext-policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, KeyGen, and Decrypt. In addition, we allow for the option of a fifth algorithm Delegate.
Setup: The setup algorithm takes no input except the implicit security parameter. It produces the public key PK and a master key MK as an output.
Data Encryption (PK, M, A): The encryption algorithm takes public key PK, a message M, and an access structure A over the set of attributes as inputs. The algorithm will encrypt the message M and outputs a ciphertext CT. The users having the set of attributes that satisfies the access structure will only be able to decrypt the message M. We assume that the ciphertext implicitly contains A.
Key Generation (MK, S): The key generation algorithm takes input as the master key MK and a set of attributes S that describe the key. It produces secret key SK as output.
Data Decryption (PK, CT, and SK): The decryption algorithm takes input such as public key PK, a ciphertext CT, which contains an access structure A, and a secret key SK, which is a secret key for a set S of attributes. If the set of attributes S satisfies the access structure A then the algorithm will decrypt the ciphertext and return a message M.
Delegate (SK, S˜): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set $S^{`}$ ⊆ S. It produces a secret key SK for the set of attributes $S^{`}$.

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 secures data retrieval issues. We 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.

REFERENCES

1. S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.
2. 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
3. M. Chuah and P. Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–6.
4. M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*, 2007, pp. 1–7.
5. R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. ACM Conf. Comput.Commun. Security*, 2007, pp. 195–203
6. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEE Symp. Security Privacy*, 2007, pp.321–334.
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. 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.
9. A. Lewko and B. Waters, "Decentralizing attribute-based encryption, "Cryptology ePrint Archive: Rep. 2010/351, 2010.
10. P. Golle, J. Staddon, M. Gagne, and P. Rasmussen, "A content-driven access control system," in *Proc. Symp. Identity Trust Internet*, 2008, pp. 26–35.
11. S. Mittra,"Iolus: A framework for scalable secure multicasting," in *Proc. ACM SIGCOMM*, 1997, pp. 277–288.33.
12. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Euro crypt*, 2005, pp. 457–473.