Volume-4, Issue-6, June-2015 • ISSN No 2277 - 8160

Research Paper Engineering

Ciphertext Policy-Attribute Based Encryption for Data Retrieval in Disruption-TolerantNetworks

C.Balakrishnan Assistant Professor S.A Engineering College Chennai, Tamil Nadu

P. Divya PG Scholar S.A Engineering College Chennai, Tamil Nadu

ABSTRACT

A military environment such as a battlefield or a hostile region is likely to suffer from temporary disconnections like jamming, environmental factors, and mobility. Disruption tolerant network [1] are the successful solution that allow wireless devices carried by soldiers to communicate with each other and access the confidential information by exploration storage nodes includes authorization policy or by updating policy .The policies include cipher- text policy attribute based encryption enables encryptors 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 . The problem of applying Cp-Abe[2] in DTN includes attribute revocation, key escrow, and coordination of attribute. In proposed system, immediately enhances backward/forward secrecy, escrows-free key issuing protocol and monotone access structure for security and efficient management in confidential data.

KEYWORDS : Attribute-basedencryption(ABE), Disruption-tolerantnetwork(DTN),Revocation key, Key authority,Securedataretrieval.

I. INTRODUCTION

A military network, suffer from major obstacles likedisconnections of wireless devices carried by soldiers to communicate with one another, sparsity of mobile nodes and energy resources.A disruption-tolerant network [1] (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact and become solutions for mobile nodes to communicate with each other in these extreme military environments. The messages between node to node may needed to wait in intermediate node for certain period of time when there is no end-to-end connection between them.

Roy [4] and Chuah [5] introduced storage nodes between the mobile nodes where data is stored or retrieved quickly and efficiently within some authorized nodes. The authorization for nodes is provided by access control policy.The data access policies are defined over user attributes or roles, which are controlled by the key authorities. The Disruption tolerant networks (DTN) architecture is used when multiple authorities manage their own dynamic attribute keys independently as a decentralized DTN [6]. For example: the attribute representing current location of moving soldiers in a battlefield or hostile region.

II. RELATED WORK

Ciphertext policy-Attribute based encryption:

CP-ABE[4] is atype of identity-based encryption with one public key and master private key used to make more restricted private keys but very expressive rules employs decryption of private keys for which ciphertextsprivate keys have "attributes" or labels and decryption policies. For working of cp-abe, list the parameters that have been configured such as users U = {u1, u2, …..,un}attributes A = {a1, a2,……, ak} and random subset of attributes have been distributed to each user D = {d1, d2,….., dx} where D ∈ A. Each user encrypt the file in a access tree T structure in which consider each leaf nodes are attributes in A and none leaf nodes is a gate node within the threshold value. The threshold ranges from kx, 0 ≤ kx≤ numxwhere numxis the numberof children for node x. The condition specification are if the node is an AND kx= numx and so if the node is an OR kx = 1.

Key policy attribute based encryption

In kp-abe, ciphertexts are labeled with a set of attributes and private keys are associated with access structures that control which ciphertext a user is able to decrypt. In this, attribute sets are used to generate ciphertexts and private keys are associated with access structures that specify which ciphertexts the user will use to decrypt. Consider a set of users U = {U1, U2,. . . ,Un}. A selection of nodes A ⊆ 2 U is known to be monotone if, for all B, C, if B ∈ A and B ⊆ C, then C ∈ A. An access structure (resp., monotonic access structure) is a gathering (resp., monotone collection) A ⊆ 2 P \ {Ø}. The sets in A are called the authenticated sets, and the sets not in A are called the unauthenticated sets.

III. CONCEPT

The problem of introducing ABE in DTN resembles in authorization and confidential problems. In which some user smays witc htheir correlated attributesatsome point(forexample, user changing their location from one region to another region), or some users secret key may be known, key revocation (or update). Nevertheless, this problem is even more problematic, in ABEschemes, sinceeachattributeissharedby multiple users due to this, anysingle userinanattributegroup woul daffecttheo the rusersinthe same group. Forexample, in an attribute group any user join sorleaves,the attributekey generatedby key authority shouldbe changedand again distributed to all othermembersinthesame group which maya ffected from bottleneck problemduringrekeying for all other users in the same group,orif any previous key is not renewed instantly security degradation problem will arise due to windows of vulnerability.

An important challenge in ABE is key escrow in which the key authority has the privilege to generate private keys for the users using the authority's master secret keys to users for specific set of at- tributes. Every key authority has the power to decrypt every ciphertext of the specific user by creating their particular attribute key due of this security problem arises (i.e.) any key authority is captured by opponent when deployed in the hostileenvironments or in the battlefield, this leads to data confidentiality and any secret element is handed over to the adversaries, this leads to data integrity or availability. It is an inherent issues even multiple security systems but it uses the asymmetric encryption system to escrows in the single-authority or multiple-authority CP-ABE. This is referenced as open pivotal problem for the military environment

The final challenge in ABE is the coordination of attributes whichare issued from multiple authorities in the attribute group. Even though multiple authorities generates and distributes attribute keys to users separately with their own master secrets, it is found to be difficult to define fine-grained(keen) access policies over attributes provided from multiple authorities. For example, suppose that attributes "user 1" and "region 1" are controlled by the key authority A, and "user 2" and "region 2" are controlled by the key authority B. Then, it becomes difficult to produce a fine grained access policy even it uses Boolean functions. OR Boolean logic in between the attributes generated from different authorities cannot be determined becausethe different authorities create their own attribute keys using their own independent and individual master secret keys. Therefore, "-out-of-" logic, cannot be expressed in the schemes.

IV. NETWORK ARCHITECTURE

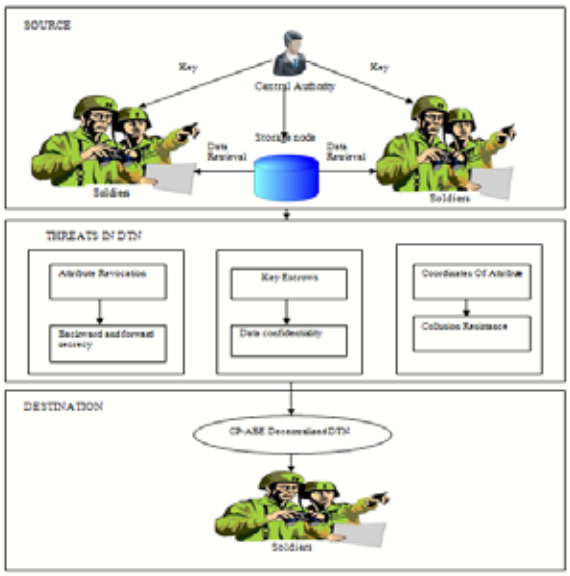

Fig.1. Architecture of CP-ABE for data retrieval in military network

System Description and assumptions

Fig. 1 shows the architecture of the CP-ABE for data retrieval. As shown in Fig. 1,the architecture consists of the following system entities.

Key Authorities: They are defined for key generation and generate public/secret parameters for CP-ABE. The key authorities play a role in two ways central authority and multiple local authorities. It provides the secure and reliable communication path between a central authority and each local authority. In this each local authority controls different attributes and provides attribute keys to users.

Storage node: This is an entity that stores data from senders and provide access to users to work on it. It may be dynamic or static. It is always assumed that storage node to be semi trusted (honest-but-curious).

Sender: This is also an entity that has the secret information or data (e.g., a commander) and it can be stored into the storage node for ease use of sharing the messages or for reliable message delivery to users in the extreme networking environments (e.g., battlefield or hostile regions). Before storing the data into the storage node the sender is responsible for defining the access policy on data by encrypting it.

User: This is a mobile node that uses the data present in the storage node (e.g., a soldier). If a user wants the data to be accessed he must satisfy the access policy of the encrypted data declared by the sender, and is not revoked in any of the attributes, and then he will be able to decrypt the ciphertext and obtain the data.

Centralized DTN: In this all or most decision makers (who have the authority, control, and responsibility for the entire organization) are located in one central office (e.g., commander) thus provides access to user in a secure way.

Decentralized DTN: In this all users have their own responsibility to access the data in a secure way.

These are applicable only if they are provided with certain access policy and within the region for security purpose.

Threat Model:

Data confidentiality: Unauthorized users who do not have enough criteria to satisfy the access policy should be stop from accessing the plain data in the storage node. Even, unauthorized access from the storage node or key authorities should be prevented.

Collusion-resistance: If the users cannot decrypt the ciphertext alone they can be able to use multiple users collude, by combining their attributes. For example, suppose there are users with attributes {"Battalion 1", "Region 1"} and another user with attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a ciphertext encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually.

In ABE, forward secrecy (FS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. Backward secrecy is presented. A security-related term, backward secrecy means that a compromise should not compromise any earlier key.

V. ALGORITHM USED

Zone based routing algorithm

ZRP[3] exploits the features of both proactive and reactive protocol. The proactive part of the protocol is restricted to a small neighbourhood of a node and the reactive part is used for routing across the network. This reduces latency in route discovery and reduces the number of control messages as well.

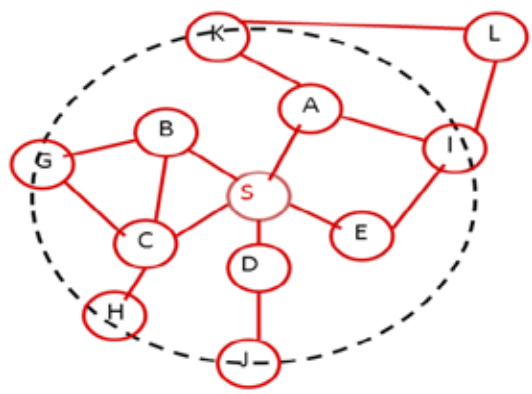

Fig.2. Architecture of ZRP

In figure 2: Each node S in the network has a routing zone. This is the proactive zone for S as S collects information about its routing zone in the manner of the DSDV protocol.

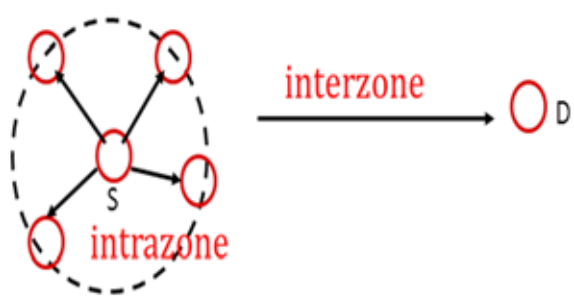

Fig.3.Intrazone and Interzone routing

In figure 3: The routing in ZRP is divided into two partsis intrazone routing and Interzone routing. First, the packet is sent within the routing zone of the source node to reach the peripheral nodes. Then the packet is sent from the peripheral nodes towards the destination node.

Fig 4. Graphical Representation

VI. CONCLUSION

Cp-abe is a scalablecryptographic solution to the access control and secures data retrieval issues. In this paper, we proposed an efficient and securedata retrieval method usingcp-abe for decentralized DTNswhere multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such thatthe confidentiality of the stored data is guaranteed even underthe hostile environment where key authorities might be fully trusted. In addition, the fine grained keyrevocation 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] JunbeomHur and Kyungtae Kang, "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" in IEEE 2014, ACM | [2]Xiaohui Liang†, Rongxing Lu†, Xiaodong Lin‡, and Xuemin (Sherman) Shen,"Ciphertext Policy Attribute Based Encryption with Efficient Revocation" in IEEE ACM. | [3] NicklasBeijar Networking Laboratory, Helsinki University of Technology, "Zone Routing Protocol (ZRP)" | [4] 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. | [5] 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. | [6] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010. |