International Journal of Engineering Innovation & Research
Volume 4, Issue 6, ISSN: 2277 – 5668

Decentralized Interruption-Tolerant using Secure Data Rescue for Armed Force Networks

Manjula HT[1], Amreen Khanam[1], Sumathi D.[1]
[1]Assistant Professor, Dept of CSE,
HKBK College of Engineering, Bangalore

***Abstract* – Mobile nodes in armed force (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 the scenario are 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.A secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently and describes how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.**

***Keywords* – Attribute-Based Encryption (ABE), Interruption-Tolerant Network (ITN), Multi Authority, Secure Data Retrieval. Disruption-Tolerant Network (DTN).**

INTRODUCTION

In many armed force(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. In many cases, it is desirable to provide differentiated 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.

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 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 encryption defines the attribute set that the decryption needs to possess in order to decrypt the cipher text. 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. 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 attribute 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 “region 2”)) 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

II. Related Works

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 giving another party your private key). We develop a new cryptosystem fore-grained sharing of encrypted data that is called Key-Policy Attribute-Based Encryption (KP-ABE) [1]. In the cryptosystem, cipher texts are labelled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.In Decentralizing Attribute-Based Encryption [2] proposes a Multi-Authority Attribute-Based Encryption (ABE) 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 in 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 assume no coordination between such authorities. Creating 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 cipher text and private keys to a semi-functional form and then arguing security.

By following a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of Composite order, proving the security under similar static assumptions to the LW paper in the random oracle model.Identity-based encryption (IBE) [3]with Efficient Revocation 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. Let us note that this solution does not scale well as the number of users increases, the work on key updates becomes a bottleneck, by proposing an IBE scheme that significantly improves key-update efficiency on the side of the trusted party, 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.Message ferrying [4] 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 it cannot be certain of the location of the nodes, and 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. presenting 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. it shows that OPWP consistently outperforms other naive ferry routing approaches.Mobile nodes in some challenging network scenariosperformance evaluations of data-centric information retrieval schemes 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 the paper it explores 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. Let us first describe how to select nodes for storing the replicated copies of data items. 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 the system, let us consider fixed, proportional and square_rootreplication schemes. Describe two query dissemination schemes: (a) W-copy Selective Query Spraying (WSS) scheme, (b) L hop Neighbourhood Spraying (LNS) scheme.

In WSN 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, it uses 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. 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 DieselNet project achieves much lower query success ratio because of the longer inter-node encounter time.

III. Existing Work

ABE comes in two flavours called key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In KP-ABE, the encryptor only gets to label a cipher text with a set of attributes. The key authority chooses a policy for each user that determines which cipher texts he can decrypt and issues the key to each user by embedding the policy into the user’s key. However, the roles of the cipher texts and keys are reversed in CP-ABE. In CP-ABE, the cipher text is encrypted with an access policy chosen by an encryptor, but a key is simply created with respect to an attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors 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.

Disadvantages of Existing Work

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 or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure.

- There is more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users.
- 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.
- 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.

IV. Proposed Work

The main objective of this proposed system is to provide the security of the network and to increase the efficiency and reliability of the network, providing Secure and reliable communication channels between a central key authority and each local authority. This proposed system enables data confidentiality and authentication for decentralised retrieval of secured data. The system provides a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme.

Since the first CP-ABE scheme proposed by Bethencourt *et al* , dozens of CP-ABE schemes have been proposed. The subsequent CP-ABE schemes are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the Bethencourt *et al.*’s scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we develop a variation of the CP-ABE algorithm partially based on (but not limited to) Bethencourt *et al.*’s construction in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from scratch.

Advantages of Proposed Work

- 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 cipher text by combining their attributes even if each of the users cannot decrypt the cipher text alone.

- Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute 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 In Proposed Work

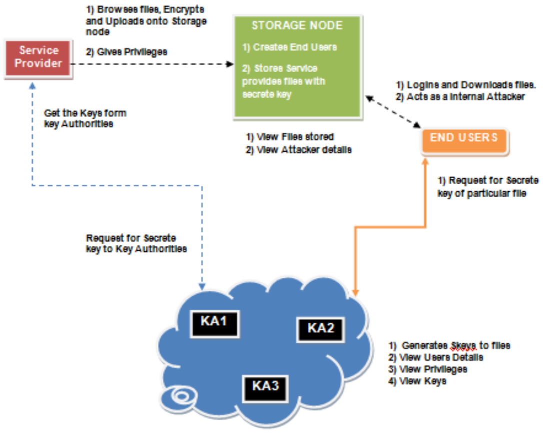
1) Browses files, Encrypts and Uploads onto Storage node
2) Gives Privileges
Service Provider
STORAGE NODE
1) Creates End Users
2) Stores Service provides files with secrete key
1) Logins and Downloads files.
2) Acts as a internal Attacker
Get the Keys form key Authorities
1) View Files stored
2) View Attacker details
END USERS
1) Request for Secrete key of particular file
Request for Secrete key to Key Authorities
KA1
KA2
KA3
1) Generates Skeys to files
2) View Users Details
3) View Privileges
4) View Keys

Fig1: Architectural diagram

Modules Used In Proposed Work

There are seven modules involved in the proposed work for secure data retrievals in disruption tolerant military network namely:

1. Key Authorities
2. Storage Nodes
3. Sender
4. User
5. Disruption Tolerant Network Router
6. End User
7. Threat model

A. 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. 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. The key authority (KA1, KA2, and KA3) is responsible to generate the secret key for the file belongs to the particular Battalion and region. The End User Request to the storage node using the file Name, secret key, Battalion and Region, Then storage node connect to the respective Key authority server. If all specified Details are correct then file will send to the end user, or else he will be blocked in a storage node. The Key Authority server can view the users, privileges, keys. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

B. 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.

C. 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. The Sender is responsible for registering the Users by providing details Name, Password, Confirm Password, Battalion (b1,b2,b3) , Region(R1,R2,R3). Sender Browses the data File, encrypts it and gets the key from Key Authority Server (KA1, KA2, and KA3). Uploads their data files to the Storage Node and sender is authenticated to provide privileges for End User.

D. 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

E. Disruption Tolerant Network Router

The Disruption Tolerant Network Router (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. In this module we 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. In DTN encrypted data file and details will be stored Storage Node.

F. End User

In this module, the End user can access the file details and end user who will request and gets file contents response from the DTN Router. If the credential file name and secret key is correct then the end user will get the file response from the router in Decrypted format.

G. Threat model

Threat model is one who is trying to access the file which is belongs to other user by injecting the fake details to the file in the storage node is considered as Attacker. The attacker can be Data confidentiality or collusion-resistance.

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

2. Collusion-resistance: Suppose there exist a user with attributes {”Battalion 1”, “Region 1”} and another user with attributes {”Battalion 2”, “Region 2”}. They may succeed in decrypting a cipher text encrypted under the access policy of (“Battalion 1” and “Region 2”), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive user keys.

H. Analysis phase

This module is to provide the security of the network and to increase the efficiency and reliability of the network, providing Secure and reliable communication channels between a central key authority and each local authority. This proposed system enables data confidentiality and authentication for decentralised retrieval of secured data. The system provides a multi authority CP-ABE scheme for secure data retrieval in decentralized DTNs. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme.

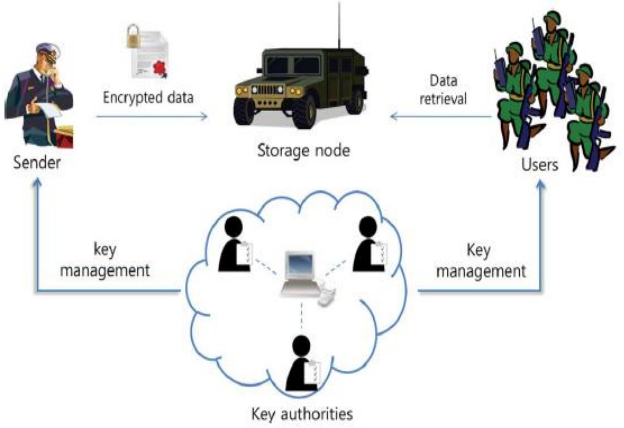

Fig.2. Architecture of secure data retrieval in adisruption-tolerant military network

V. Conclusion and Future Enhancement

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.

The future work that can be done by adding mail facilities and chat box for emergency purpose for users when they are under blocked status, that can further be enhanced in banking sectors, industrial sector and forests applications where confidentiality is the prime priority.

References

[1] Vipul Goyal, Omkant Pandey, Amit Sahai Brent, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”

[2] J.Burgess,B. Gallagher, D. Jensen, and B. N. Levine, “Decentralizing Attribute-Based Encryption,”in*Proc. IEEE INFOCOM*, 2006.

[3] M. Chuah and P. Yang, “Identity-based Encryption with Efficient Revocation,” in *Proc. IEEE MILCOM*, 2006, pp. 1–6.

[4] M. M. B. Tariq, M. Ammar, and E. Zequra, “Mesage ferry route design for sparse adhoc networks with mobile nodes,” in *Proc. ACM MobiHoc*, 2006, pp. 37–48

[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] S. Roy andM. Chuah, “Secure data retrieval based on ciphertext policy attribute-based encryption(CP-ABE) system for the DTNs,” LehighCSEh. Rep., 2009.

[7] 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.

[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker,“Mediated cipher text-policyattribute-based encryption and its application,” in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[9] 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.

[10] D.Huang and M. Verma, “ASPE: Attribute-based secure policyenforcementin vehicular ad hoc networks,” Ad Hoc Netw., vol. 7, no. 8, pp. 1526–1535,2009.

[12] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc.Eurocrypt, 2005, pp.457-473.

Author's Profile

Manjula HT

received the B.E. degree in information Science and Engineering from Visvesvaraya Technological University, Belagavi, Karnataka in 2008 and M.Tech. degree in computer science and engineering from Visvesvaraya Technological University, Belagavi, Karnataka in 2010. Currently working as Asst. professor in HKBKCE, Bangalore.

Amreen Khanam

received the B.E. degree in computer science engineering from Visvesvaraya Technological University, Belagavi, Karnataka in 2009 and pursuing M.Tech. degree from Visvesvaraya Technological University, Belagavi, Karnataka. Currently working as Asst. professor in HKBKCE, Bangalore.

Sumathi D.

received the B.E. degree in computer science engineering from, Manonmaniamsundaranar University, Tirunelveli in 2001 and ME degree in computer science engineering from Bangalore University, Karnataka in 2013.Currently working as Asst. professor in HKBKCE, Bangalore.