ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 8, August 2015

Dynamically Secure Data Sending To Military Networks in DTNs

Subhashini.V, Bullarao Domathoti, Nageswara Rao Putta

M. Tech, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India.

Assistant Professor, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India.

Associate Professor, Dept. of CSE., SITS, JNT University, Aanthapur, Tirupati, AP, India.

ABSTRACT: Mobile nodes in military environments like a tract or a hostile region square measure seemingly to suffer from intermittent network property and frequent partitions. Disruption-tolerant network (DTN) technologies are getting undefeated solutions that permit wireless devices carried by troopers to speak with one another and access the lead or command dependably by exploiting storage device nodes. Disruption- tolerant network (DTN) technologies are getting undefeated solutions that permit nodes to speak with one another in these extreme networking environments. Typically, once there's no end-to-end affiliation between a supply and a destination try, the messages from the supply node might have to attend within the intermediate nodes for a considerable quantity of your time till the affiliation would be eventually established. The idea of attribute-based encoding (ABE) could be a promising approach that fulfills the wants for secure information retrieval in DTNs. Especially, Cipher text-Policy ABE (CP-ABE) provides a scalable means of encrypting information such the encryptor defines the attribute set that the decodeor must possess so as to decrypt the cipher text. Thus, totally different completely different} users square measure allowed to decode different items of knowledge per the protection policy.

KEYWORDS: Access control; attribute-based encryption (ABE); disruption-tolerant network(DTN); multi authority; secure data retrieval;

I. 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 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 a 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 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 (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 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. 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.

II. Related work

ABE comes in two flavors 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 [4], [7], [15]. 1) Attribute Revocation: Be then court et al. [13] and Boldyrevaetal.[16] first suggested key revocation mechanisms in CP-ABE and KP-ABE, respectively. Their solutions are to append to each attribute an expiration date (or time) and dis- tribute an ew set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes [8], [13], [16], [17] have two main problems. The first problem is the security degradation in terms of the backward and forward secrecy [18]. 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[4],[9].

Then, a user who newly holds the attribute might be able to access the previous data encrypted before he obtains the attribute until the data is re encrypted with the newly Updated attribute keys by periodicre keying (backward secrecy). For example, assume that at time ,a cipher text is encrypted with a policy that can be decrypted with a set of attributes (embedded in the users keys) for users with .Aftertime ,say , a user newly holds the attribute set . Even if the new user should be disallowed to decrypt the cipher text for the time instance , he can still decrypt the previous cipher text until it is re encrypted with the newly updated attribute keys. On the other hand, a revoked user would still be able to access the en- crypted data even if he does not hold the attribute any more until the next expiration time (forward secrecy). For example, when a user is disqualified with the attribute at time he can still decrypt the cipher text of the previous time instance unless the key of the user is expired and the cipher text is re encrypted with the newly updated key that the user cannot obtain. We call this un controlled period of time windows of vulnerability. 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- ” problem, which means that the update of a single attribute affects the whole n on revoked users who share the attribute[19].This could be a bottleneck for both the key authority and all non revoked users. The immediate key revocation can be done by revoking users using ABE that supports negative clauses [4], [14]. To do so, one just adds conjunctively the AND of negation of revoked user identities (where each is considered as an attribute here). However, this solution still somewhat lacks efficiency performance. This scheme will pose overhead groupelements1 additively to the size of the cipher text and multiplicatively to the size of private key over the original CP-ABE scheme of Be then court et al. [13], where is the maximum size of revoked attributes set. Golleetal.[20] also proposed a user revocable KP-ABE scheme, but their scheme only works when the number of attributes associated with a cipher text is exactly half of the universe size.

2) KeyEscrow:

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 [11], [13], [14], [21]–[23]. Thus, the key escrow problem is inherent such that the key authority can decrypt every cipher text addressed to users in the system by generating their secret keys at any time. Chaseetal. [24] presented a distributed KP-ABE scheme that solves the key escrow problem in a multi authority 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. One disadvantage of this fully distributed approach is the performance degradation. Since there is no centralized authority with master secret information, all attribute authorities should communicate with each other in the system to generate a user's secret key.

III. Proposed algorithm

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. 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.

A. *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.

B. ***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.

C. ***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.

D. ***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.

E. *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.

F. *System Description and Assumptions:*

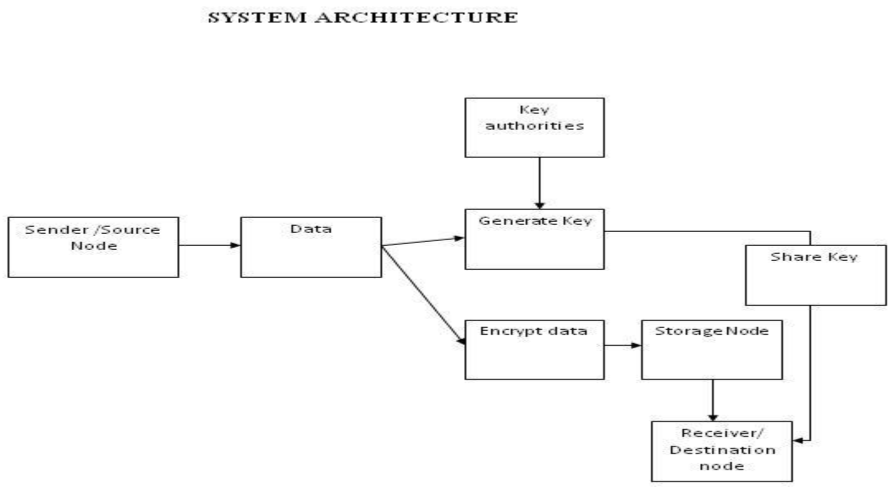
SYSTEM ARCHITECTURE

Fig.1shows the architecture of the DTN . As shown ing Fig.1, the architecture consists of the following system entities. 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 at- tributes 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 mo- bile or static [4], [5]. 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) 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 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. Si

G. *Contribution*

In this paper, we propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. 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, encrypt or scan define a finegrained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is re- solved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. 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. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy can be crypto- graphically enforced against any curious key authorities or data storage nodes in the proposed scheme.

IV. SIMULATION RESULTS

we analyze and measure the computation cost for en- crypting (by a sender) and decrypting (by a user) a data. Microsoft .NET is a set of Microsoft software technologies for rapidly building and integrating XML Web services, Microsoft Windows-based applications, and Web solutions. The .NET Framework is a language-neutral platform for writing programs that can easily and securely interoperate. There’s no language barrier with .NET: there are numerous languages available to the developer including Managed C++, C#, Visual Basic and Java Script. The .NET framework provides the foundation for components to interact seamlessly, whether locally or remotely on different platforms. It standardizes common data types and communications protocols so that components created in different languages can easily interoperate.

“.NET” is also the collective name given to various software components built upon the .NET platform. These will be both products (Visual Studio.NET and Windows.NET Server, for instance) and services (like Passport, .NET My Services, and so on).

In this simulation, we consider DTN applications using the Internet protected by the attribute-based encryption. Almeroth and Anmar [3] demonstrated the group behavior in the Internet’s multicast backbone network (MBone). They showed that the number of users joining a group follows a Poisson distribution with rate ,and the membership duration time follows an exponential distribution with a mean duration . Since each attribute group can be shown as an independent network multicast group where the members of the group share a common attribute, we show the simulation result following this probabilistic behavior distribution [3].

The membership duration time for an attribute is assumed to follow an exponential distribution. We set the interarrival time between users as 20 min(λ=3) and the average membership duration time as 20h.

DOI: 10.15680/IJIRCCE.2015. 0308020

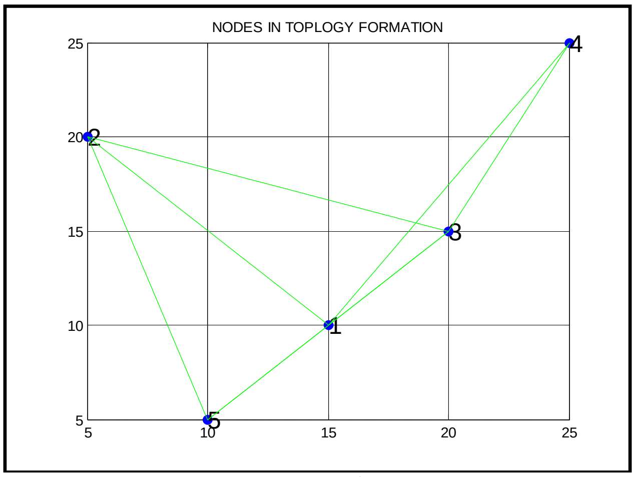

Fig.1. Ad Hoc Network of 5 Nodes

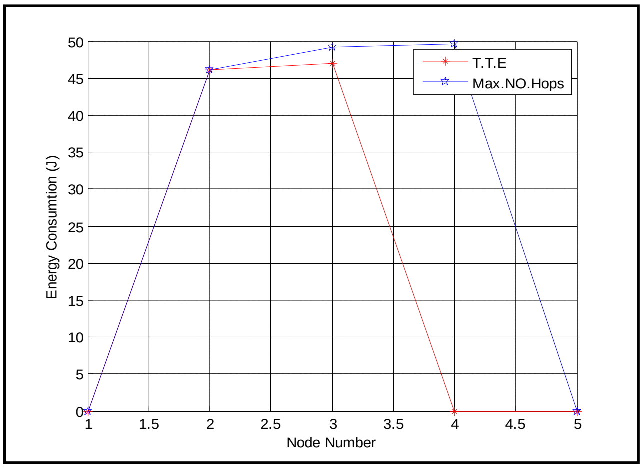

Fig. 2. Number of users in an attribute group.

Next, we analyze and measure the computation cost for en- crypting (by a sender) and decrypting (by a user) a data. We used a Type Acurve (in the pairing based cryptography(PBC) library[33]) providing groups in which a byline a map is defined. Although such curves provide good computational efficiency (especially for pairing computation), the same doesnot hold from the point of view of the space required to represent group elements. Indeed, each element of needs 512 bits at an 80-bit security level and 1536 bits when 128-bit of security are chosen. Table III shows the computational time results. For each op- eration, we include a bench mark timing. Each crypto graphic operation was implemented using the PBC libraryver.0.4.18[33] ona3.0-GHzprocessorPC.Thepublickeyparameterswereselectedtoprovide80-bitsecuritylevel.Theimplementationuses a 160-bit elliptic curve group based on the supersingular curve overa512-bitfinitefield.Thecomputationalcost is analyzed in terms of the pairing, exponentiation operations in and . The comparatively negligible hash, symmetric key, and multiplication operations in the group are ignored in the time result. In this analysis, we assume that the access tree in the ciphertext is a complete binary tree. Computation costs in Table III represent the upper bound of each cost. We can see that the total computation time to en- crypt data by a sender in the proposed scheme is the same as BSW, while decryption time by a user requires exponentiations in more. These exponentiation operations are to realize the fine-grained key revocation for each attribute group. Therefore, we can observe that there is a trade off between computational overhead and granularity of access control, which is closely related to the windows of vulnerability. However, the computation cost for encryption by a sender and decryption by a user are more efficient compared to the other multi authority schemes.

V. CONCLUSION AND FUTURE WORK

The 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 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. Anjum Asma and Gihan Nagib,'Energy Efficient Routing Algorithms for Mobile Ad Hoc Networks–A Survey', International Journal of Emerging Trends & Technology in computer Science, Vol.3, Issue 1, pp. 218-223, 2012.
2. Hong-ryeol Gil1, Joon Yoo1 and Jong-won Lee2 ,'An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks', Proceedings of the 2nd International Conference on Human. Society and Internet HSI'03, pp. 302-311, 2003.

3. S.K. Dhurandher, S. Misra, M.S. Obaidat, V. Basal, P. Singh and V. Punia,'An Energy-Efficient On Demand Routing algorithm for Mobile Ad-Hoc Networks', 15 th International conference on Electronics, Circuits and Systems, pp. 958-9618, 2008.
4. DilipKumar S. M. and Vijaya Kumar B. P. ,'Energy-Aware Multicast Routing in MANETs: A Genetic Algorithm Approach', *International Journal of* Computer *Science and Information Security* (IJCSIS), Vol. 2, 2009.
5. AlGabri Malek, Chunlin LI, Z. Yang, Naji Hasan.A.H and X.Zhang ,' Improved the Energy of Ad hoc On- Demand Distance Vector Routing Protocol', International Conference on Future Computer Supported Education, Published by Elsevier, IERI, pp. 355-361, 2012.
6. D.Shama and A.kush,'GPS Enabled E Energy Efficient Routing for Manet', International Journal of Computer Networks (IJCN), Vol.3, Issue 3, pp. 159-166, 2011.
7. Shilpa jain and Sourabh jain ,'Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)', international Journal of Computer Networks and Wireless Communications, Vol.2, Issue 4, pp. 450-455, 2012.
8. Vadivel, R and V. Murali Bhaskaran,'Energy Efficient with Secured Reliable Routing Protocol (EESRRP) for Mobile Ad-Hoc Networks', Procedia Technology 4,pp. 703- 707, 2012.