International Journal of Computer Applications Technology and Research
Volume 4– Issue 5, 368 - 373, 2015, ISSN:- 2319–8656

Military Networks by Disruption Tolerant Network Technology

K.V Srikanth
Dept. Of C.S.E.
Bharath University
Chennai, India

B.Aravindsamy
Dept. Of C.S.E.
Bharath University
Chennai, India

S.Pothumani
Dept. Of C.S.E.
Bharath University
Chennai, India

Abstract: Mobile nodes in military environments like a field of battle or a hostile region ar seemingly to suffer from intermittent network property and frequent partitions. Disruption-tolerant network (DTN) technologieshave become eminent solutions that enable wireless devices carried by troopers to speak with one another and access the guidance or command faithfully by exploiting secondary storage nodes.a number of the foremost difficult problems during this state of affairs ar the social control of authorization policiesand also the policies update for secure information retrieval. Ciphertext- policy attribute-based secret writing (CP-ABE) could be a promising cryptologic resolution to the access management problems. However, the matter of applying CP-ABE in suburbanised DTNs introduces many security and privacy challenges with respect to the issued fromtotally different authorities. during this paper, we have a tendencyto propose se- cure information retrieval theme victimization CP-ABE for suburbanised DTNs wherever multiple key authorities manage their attributes severally. we have a tendency to demonstrate a way to apply the projected mechanism and with efficiency manage confidential information distributed within the disruption-tolerant military network.

Keyworsds: DTN- Disruption tolerant network, CP-ABE- Cipher text-Policy Attribute-Based Encryption, IBE- Identity Based Encryption2 PC-Protocol To Protocol, PKI-Public Key Infrastructure, ACG-Access Control Gadgets , DBDH- Decision Bilinear Diffie Hellman assumption, KGC-Key Generative Center.

I.INTRODUCTION

In several military network troopers is briefly disconnected by jam,environmental. Disruption-tolerant network (DTN) technologies have become successful solutions that enable nodes to speak with one another in these extreme networking access services specified knowledge access policies are outlined over user attributes or roles that are managed by disruption-tolerant military network, a commander might store a counseling at a 1" United Nations agency are taking part in "Region two." during this case, it's an inexpensive assumption that multiple key authorities are possible to manage their own dynamic attributes for troopers in their deployed regions or echelons, (ABE) [11]–[14] could be a promising approach that fulfills the wants forse-cure knowledge retrieval in DTNs. ABE options a mechanism that allows associate degree access management over encrypted knowledge exploitation access policies and ascribed attributes among personal keys and ciphertexts. Especially, ciphertext-policy ABE (CP-ABE) provides a scalable method of encrypting knowledge specified the encryptor defines the attribute set that the decryptor must possess so as to de-crypt the ciphertext [13].. However, the matter of applying the ABE to DTNs introduces many security their associated attributes at some purpose (for ex-ample, moving their region), or some personal keys could be compromised, key revocation (or update) for every attribute is in any single user in an attribute cluster would have an effect on the opposite users within the cluster. For ex-ample, if a user joins or leaves associate and decentralized to all or any the opposite members within the same cluster for backward or rekeying procedure, or security degradation as a result of the windows of vulnerability if the previous attribute key's not updated directly.

2. LITERATURE SURVEY

Identity-Based Encryption With Efficient Revocation, Identity-based encryption (IBE) is an exciting alternative to public-key encryption, as IBE eliminates the need for a Public Key Infrastructure (PKI). PKI- or identity-based, Its provide a revoke users from the system. Efficient revocation is a well-studied problem in the traditional PKI setting. The setting of IBE 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. That this solution does not scale well – as the number of user's increases, the work on key updates becomes a bottleneck.

Decentralizing Attribute-Based Encryption, 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 that react 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 .We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

User-Driven Access Control: Rethinking Permission Granting In Modern Operating Systems, Modern client platforms, such as iOS, Android, Windows Phone, Windows 8, and web browsers, run each application in an isolated environment with limited privileges. A pressing open problem in such systems is how to allow users to grant applications access to user-owned resources, e.g., to privacy- and cost-sensitive devices like the camera or to user data residing in other applications. A key challenge is to enable such access in a way that is non-disruptive to users while still maintaining least-privilege restrictions on applications To allow the system to precisely capture permission-granting intent in an application's context, we introduce access control gadgets (ACGs). Each user-owned resource exposes ACGs for applications to embed. The user's authentic UI interactions with an ACG grant the application permission to access the corresponding resource. Our prototyping and evaluation experience indicates that user driven access control enables in-context, non-disruptive, and least-privilege permission granting on modern client platforms.

Efficient And Provable Secure Cipher Text-Policy Attribute-Based Encryption Schemes, In CP-ABE scheme, the data is encrypted under an access policy defened by a user who encrypts the data and a user secret key is associated with a set of at- tributes which identify the user. A user can decrypt the ciphertext if and only if his attributes satisfy the access policy. In CP-ABE, the user enforces the access policy at the encryption phase, the policy moves with the encrypted data. It's important for data storage servers where data confidentiality must be preserved even if the server is compromised or un-trusted. The scheme is secure under Decision Bilinear Diffie Hellman assumption (DBDH). The expressivity of the scheme by including of (threshold) operator in addition to and operators. Comparison with existing CP-ABE schemes and show that our schemes are more efficient .The computational work done by the decryptor is reduced.

Selective Group Broadcast In Vehicular Networks Using Dynamic Abe ,CP-ABE) provides an encrypted access control mechanism for broadcasting messages. Basically, a sender encrypts a message with an access control policy tree which is logically composed of attributes; receivers are able to decrypt the message when their attributes satisfy the policy tree. A user's attributes stand for the properties that he current has. It is required for a user to keep his attributes up-to-date. It is difficult in CP-ABE because one attribute changes, the entire private key, which is based on all the attributes, must be changed .We introduce fading function, which renders attributes "dynamic" and allows us to update each one of them separately .Choosing fading rate for fading function affects the efficiency and security. We also compare our design with CP-ABE and find our scheme performs significantly better under certain circumstance.

3. RELATED WORK:

ABE comes in 2 flavors known as key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the encryptor solely gets to label a ciphertext with a collection of attributes. However, the roles of the cipher texts and keys square measure reversed in CP -ABE. In CP-ABE, the ciphertext is encrypted with AN access policy chosen by AN encryptor, however a key's merely created with regard to an attributes set. CP-ABE is additional acceptable to DTNs than KP-ABE as a result of it allows en cipherors like a commander to settle on AN access policy on attributes and to encrypt confidential information below the access structure via encrypting with the corresponding public keys or attributes .

1).Attribute Revocation:

Bethencourt et al. [13] and Boldyreva et al. [16] 1st recommended key revocation mechanisms in CP-ABE and KP-ABE, severally. Their solutions area unit to append to every attribute Associate in Nursing expiration date (or time) and distribute a brand new set of keys to valid users once the expiration.The first drawback is that the security degradation in terms of the backward and forward secrecy it's a substantial scenario that users like troopers could amendment the attributes frequently, Then, a user World Health Organization freshly holds the attribute could be able to access the previous knowledge encrypted before he obtains the attribute till the info is re-encrypted with the freshly updated attribute keys by periodic rekeying (backward secrecy). as an example, assume that may be decrypted with a collection of attributes (embedded within the users keys) for users with . After time , say , a user freshly holds the attribute set . albeit the new user ought to be disallowed to decipher the ciphertext for the time instance , he will still decipher the previous ciphertext till it's re-encrypted with the freshly updated attribute keys. On the opposite hand, a revoked user would still be able to access the encrypted knowledge albeit he doesn't hold the attribute any further till successive expiration time (forward secrecy).

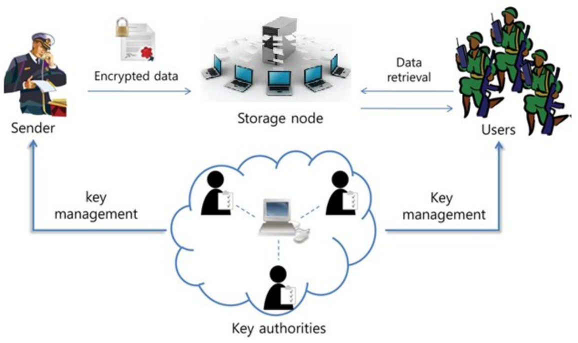
2). *Key Escrow:*

Most of the present ABE schemes square measure constructed on the design wherever one trusty authority has the ability to get the complete non-public keys of users with its master secret info[11], [13], [14], [21]–[23]. Thus, the key written agreement drawback is inherent specified the key authority will rewrite each ciphertext addressed to users within the system by generating their secret keys at anytime. Chase et al. [24] bestowed a distributed KP-ABE theme that solves the key written agreement drawback in an exceedingly multi authority system. During this approach, all (disjoint) attribute authorities square measure collaborating within the key generation protocol in an exceedingly distributed method specified they cannot pool their information and link multiple attribute sets happiness to a similar user. One disadvantage of this totally distributed approach is that the performance degradation. Since there's no centralized authority with master secret info, all attribute authorities ought to communicate with one another within the system to get a user's secret key. This ends up in communication overhead on the system setup and therefore the rekeying phases and needs every user to store further auxiliary key elements besides the attributes keys, wherever is that the variety of authorities within the system.

3. *) Decentralized ABE:*

Huang and Roy et al. [4] projected decentralized CP-ABE schemes within the multi authority network surroundings. They achieved a combined access policy over the attributes issued from completely different authorities by merely encrypting information multiple times. the most disadvantages of this approach area unit potency and quality of access policy. for instance, once a commander encrypts a secret mission to troopers beneath the policy it can not be expressed once every "Region" attribute is managed by completely different authorities, since merely multi encrypting approaches will by no means that specific any general . Therefore, they're somewhat restricted in terms of quality of the access policy and need computation and storage prices. Chase and Lewko et al. [10] projected multi authority KP-ABE and CP-ABE schemes, severally. However, their schemes additionally suffer from the key written agreement drawback just like the previous decentralized

4. NETWORK ARCHITECTURE



In this section, we describe the DTN architecture and define the security model

Fig. 1. Architecture of secure data retrieval in a disruption-tolerant military network *System Description and Assumptions.*

1) Key Authorities: they're key generation centers that generate public/secret parameters for CP-ABE. The key authorities comprises a central authority and multiple native authorities. we tend to assume that there are secure and reliable communication channels between a central authority and every bureau throughout the initial key setup and generation section. They grant differential access rights to individual users supported the users' attributes. The key authorities are assumed to be honest-but-curious. That is, they're going to honestly execute the allotted tasks within the system, but they might prefer to learn data of encrypted contents the maximum amount as potential.

2) Storage Node: this is often associate degree entity that stores knowledge from senders and supply corresponding access to users. it's going to be mo-bile or static [4], [5]. almost like the previous schemes, we tend to additionally assume the storage

node to be semi trusted , that's honest-but-curious.

3)Sender: This is often associate degree entity World Health Organization owns confidential messages or knowledge (e.g., a commander) and needs to store them into the external knowledge storage node for simple sharing or for reliable delivery to users within the extreme networking environments. A sender is chargeable for shaping (attribute-based) access policy and implementing it on its own

4) User: this is often a mobile node World Health Organization needs to access the info keep at the storage node (e.g., a soldier). If a user possesses a collection of attributes satisfying the access policy of the encrypted knowledge outlined by the sender, and isn't revoked in any of the attributes, then he are going to be ready to rewrite the cip her text and procure the info.

5. ANALYSIS

In this section, we have a tendency to first analyze and compare the efficiency of the projected theme to the previous multi authority CP-ABE schemes in theoretical aspects. Then, the potency of the projected theme is incontestable within the network simulation in terms of the communication value . we have a tendency to additionally discuss its potency once enforced with specific parameters and compare these results to those obtained by the opposite schemes.

A.Efficiency:

Logic expressiveness of access structure which will be outline dunderneath totally {different |completely different} disjoint sets of attributes (managed by different authorities), key escrow, and revocation roughness of every CP-ABE theme. within the projected theme, the logic are often terribly communicative as within the single authority system like BSW [13] specified the access policy are often expressed with any monotone access structure underneath attributes of any chosen set of authorities; whereas HV [9] and RC [4] schemes solelyenable the gate among the sets of attributes managed by completely different authorities. The revocation within the projected theme are often wiped out an on the spot method as against BSW. Therefore, attributes of users are often revoked at any time even before the expiration time that may be set summarizes the potency comparison results among CP-ABE schemes. within the comparison, rekeying message size represents the communication price that the key authority or the storage node has to send to update non-revoked users' keys for associate attribute. non-public key size represents the storage price required for every user to store attribute keys or KEKs. Public key size represents the scale of the system public parameters. during this comparison, the access tree is built with attributes of completely different authorities except in BSW of that total size is capable that of the one access tree in BSW. As shown in Table II, the projected theme desires rekeying message size of at the most to notice user-level access management for every attribute within the system .though RC doesn't got to send extra rekeying message for user revocations as against the opposite schemes, its cip her text size is linear to the quantity of revoked users within the system since the user revocation message is enclosed within the cip her text. The projected theme needs a user to store additional KEKs than BSW. However, it's a sway on reducing the rekeying message size. The projected theme is as economical because the basic BSW in terms of the cip her text size where as realizing safer immediate rekeying in multi-authority systems.

B. Simulation:

In this simulation, we have a tendency to take into account DTN applications victimisation the net protected by the attribute-based cryptography. Almeroth and Anmar [32] incontestable the cluster behavior within the Internet's multicast backbone network (MBone). They showed that the quantity of users change of integrity a bunch follows a Poisson distribution with rate , and therefore the membership length time follows Associate in Nursing exponential distribution with a mean length . Since every attribute cluster may be shown as Associate in Nursing freelance network multi cast cluster wherever the members of the cluster share a typical attribute, we have a tendency to show the simulation result following this probabilistic behavior distribution.

The amount of the key authorities is ten, and therefore the average variety of attributes related to a user's secret is ten. For a good comparison with relevancy the safety perspective, we have a tendency to set the rekeying periods in HV as min. to attain associate degree 80-bit security level, we set . isn't additional to the simulation result as a result of it's common altogether multi authority CP-ABE schemes. As shown in Fig. 3, the communication value in HV is a smaller amount than RC within the starting of the simulation time (until regarding thirty h). However, because the time elapses, it will increase prominently as a result of the amount of revoked users will increase accumulatively. The projected theme needs the smallest amount communication value within the network system since the rekeying message in is comparatively but the opposite multi authority schemes.

C. Implementation:

Next, we tend to analyze and live the computation price for encrypting (by a sender) and decrypting (by a user) an information. we tend to used a Type- A curve (in the pairing-based cryptography (PBC) library [33]) providing teams within which a additive map is outlined . Though such curves give smart computational efficiency (especially for pairing computation), an equivalent doesn't hold from the purpose of read of the area needed to represent cluster components .The implementation uses a 160-bit elliptic curve cluster supported the super singular curve over a 512 -bit finite field. The process price is analyzed in terms of the pairing, involution operations in and the relatively negligible hash, cruciform key, and multiplication operations within the cluster square measure unheeded within the time result. during this analysis, we tend to assume Computation prices in Table III represent the edge of every price. we are able to see that the overall computation time to encrypt knowledge by a sender within the planned theme is that the same as BSW, whereas coding time by a user needs exponentiations in a lot of.

6. SECURITY

In this section, we prove the security of our scheme with regard to the security requirements discussed.

A. Collusion Resistance:

In CP-ABE, the key sharing should be embedded into the cip her text instead to the non-public keys are irregular with personalized random values selected by the such they can't be combined within the projected scheme .This price are often blind out if and providing the user has the enough key parts to satisfy the key sharing theme embedded within the cip her text. Another collusion attack state of affairs is that the collusion between revoked users so as to obtain the valid attribute cluster keys for a few attributes that they're not licensed to possess (e.g., because of revocation). The at-tribute cluster key distribution protocol, that is complete sub-tree methodology within the projected theme, is secure in terms of the key identity [29]. Thus, the colluding revoked users will by no suggests that get any valid attribute cluster keys for at-tributes that they're not licensed to carry. Therefore, the colluding native authorities cannot derive the total set of secret keys of users.

B *Data Confidentiality:*

In our trust model, the multiple key authorities are not any longer absolutely trustworthy further because the storage node even though they're honest Data confidentiality on the keep knowledge against unauthorized users are often trivially warranted. If the set of attributes of a user cannot satisfy the access tree within the cip her text, he cannot recover the specified price throughout the secret writing method, wherever could be a random price unambiguously assigned to him. On the opposite hand, once a user is revoked from some attribute teams that satisfy the access policy, he cannot rewrite the cip her text either unless the remainder of the attributes of him satisfy the access policy. so as to rewrite a node for AN attribute , the user mustry from the cip her text and from its personal key. However, this cannot end in the worth , that is desired to get , since is blind by the updated attribute cluster key that the revoked user from the attribute cluster will by no suggests that get.

B. Backward and Forward Secrecy:

When a user involves hold a collection of attributes that satisfy the access policy within the cip hertext at your time instance, the corresponding attribute cluster keys are updated and delivered to the valid attribute cluster members firmly (including the user). Additionally, all of the element sencrypted with a secret key within the cip her text are re-encrypted by the storage node with a random ,and also the cip her text elements reminiscent of the attributes are re-encrypted with the updated attribute cluster keys. even though the user has keep the previous cip hertext exchanged before he obtains the attribute keys and also the holding at-tributes satisfy the access policy, he cannot re-write the pervious cip her text. this can be as a result of, even though he will reach computing from the present cip her text, it'll not facilitate to recover the specified price for the previous cip her text since it's unsighted by a random .On the opposite hand, once a user involves drop a collection of at-tributes that satisfy the access policy at your time instance, the corresponding attribute cluster keys are updated and delivered to the valid attribute cluster members firmly (excluding the user). Then, all of the elements encrypted with a secret key within the cip her text are re encrypted by the storage node with a random , and also the cip hertext elements reminiscent of the attributes are re encrypted with the updated attribute cluster keys.

7. CONCLUSION

DTN technologies have become self-made solutions in military applications that permit wireless devices to speak with one another and access the counseling reliably by exploiting storage device nodes. CP-ABE could be a scalable science resolution to the access management and secure information retrieval problems .During this paper we tend to planned Associate in Nursing economical and secure information retrieval technique victimization CP-ABE for localized DTNs wherever multiple key authorities manage their attributes independently. The inherent key written agreement drawback is resolved specified the confidentiality of the hold on information is secure deven underneath the hostile atmosphere wherever key authorities could be com-promised or not totally trust worthy . Additionally, the fine -grained key revocation are often finished every attribute cluster. we tend to demonstrate the way to apply the planned mechanism to firmly and expeditiously manage the confidential information distributed within 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 de-sign for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc*, 2006, pp. 37–48.

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. 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,
    a. 1526–1535, 2009.
10. A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

11. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Eurocrypt*, 2005, pp. 457–473.

12. 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.

13. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334.

14. 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.

15. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *Proc. ASIACCS*, 2010, pp. 261–270.

16. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proc. ACM Conf. Comput. Commun. Security*, 2008, pp. 417–426.

17. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *Proc. ACM Conf. Comput. Commun. Security*, 2006,

18. 28 M.Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss,A.Hysyanskaya, and H. Shacham, "Randomizable proofs and delegatable anonymous credentials," in *Proc. Crypto*, LNCS 5677, pp. 108–125.

19. 29D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proc. CRYPTO*, 2001, LNCS 2139, pp.41–62.

20. 30C. K.Wong,M. Gouda, and S. S. Lam, "Secure group communications using key graphs," in *Proc. ACM SIGCOMM*, 1998, pp. 68–79.