https://dx.doi.org/10.22161/ijaers/3.10.11 *ISSN: 2349-6495(P) | 2456-1908(O)*

Secured Decentralized Confidential Data Distributed in the Disruption-Tolerant Military Network

Aniruddha Singh Chauhan[1], Prof. Nikita Umare[2]

[1]ME 3rd Sem. WCC Student, Abha Gaikwad-Patil College of Engineering, Nagpur, India
[2]Department of CSE/WCC, Abha Gaikwad-Patil College of Engineering, Nagpur, India

Abstract— *Disruption tolerant network 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 this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. We propose a secure data retrieval scheme using idea for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.*

Keywords—Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN).

I. INTRODUCTION

Mobile nodes in 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 in this extreme networking environment typically when there is no end to end connection between source and destination pairs, 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. Storage nodes in DTNs where data is stored or replicated in a way 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 and provide differentiated access service such that data access policies, which are defined as per user attributes or roles, which are managed by the key authorities and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the 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.

However, the problem of applying CP ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. We propose a secure data retrieval scheme using CPABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

II. PROBLEM DEFINITION

Military applications require increased protection of confidential data including access control method 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.

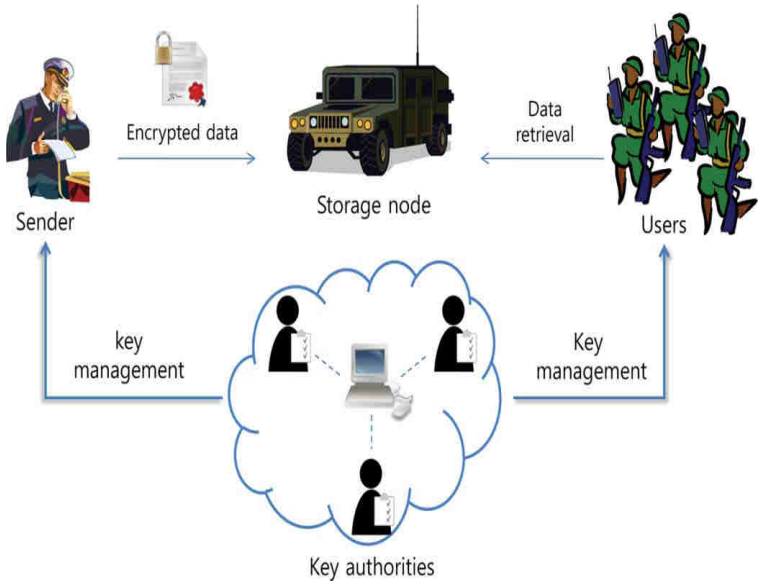


Fig.1: System Flow

https://dx.doi.org/10.22161/ijaers/3.10.11 *ISSN: 2349-6495(P) | 2456-1908(O)*

III. PROPOSED METHOD

1) Key Authorities: They are key generation centres that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. 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 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 entity stores data from senders and provide corresponding access to users. It may be mobile or static, we also assume the storage node to be semi trusted, that is honest-but-curious.

3) Sender: This entity 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 mobile node 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 and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; meanwhile, they should be still able to issue secret keys to users.

In order to realize this contradictory requirement, the central authority and the local authorities engage in the arithmetic 2PC protocol with master secret keys of their own and issue independent key components to users during the key issuing phase.

The 2PC protocol prevents them from knowing each other's master secrets so that none of them can generate the whole set of secret keys of users individually. Thus, we take an assumption that the central authority does not collude with the local authorities (otherwise, they can guess the secret keys of every user by sharing their master secrets).

Problems in Proposed Method:

1) 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 [11]–[13]. For example, 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 users' keys

2)Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) 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.

3) Key Escrow: 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 adversaries when deployed in the hostile environments compromise the key authority, 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.

IV. REASERCH CONTRIBUTION

Technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Cipher text-policy attribute-based encryption is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities.

Hence, we propose a secure data retrieval scheme using IDEA Algorithm as 3DES with MD5 Algorithm Known as Crypto Hybrid Algorithm for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

https://dx.doi.org/10.22161/ijaers/3.10.11 *ISSN: 2349-6495(P) | 2456-1908(O)*

3DES with MD5 ALGORTHIM

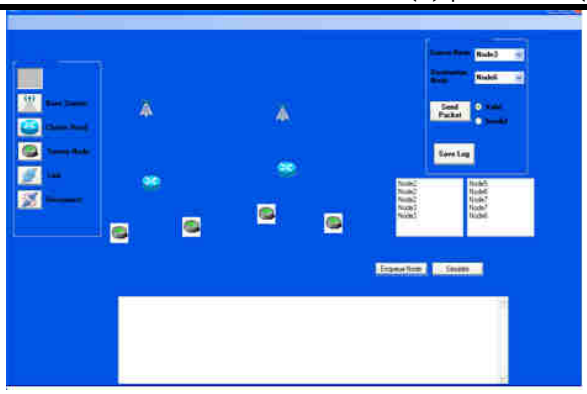
Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. Triple DES is simply another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Private Encryption, you simply type in the entire 192-bit key rather than entering each of the three keys individually. The Triple DES then breaks the user provided key into three sub keys, padding the keys if necessary so they are each 64 bits long. The procedure for encryption is the same as regular DES, but it is repeated three times. Hence, the name Triple DES, The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES, also known as 3DES.

Consequently, Triple DES runs three times slower than standard DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Unfortunately, there are some weak keys that one should be aware of: if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is essentially the same as standard DES. This situation is to be avoided because it is the same as using a slow version of regular DES.

Note that although the input key for DES is 64 bits long, the actual key used by DES is only 56 bits in length. The least significant (right most) bit in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because each of the three keys contains 8 parity bits that are not used during the encryption process.

A commonly used technique in the Internet is to provide a MD5 -Hash String so the receiver can compare if the file has been transmitted without any modifications.

3DES encrypts a 64-bit block of plaintext to 64-bit block of ciphertext. It uses a 128-bit key. The algorithm consists of eight identical rounds and a “half” roundfinal Transformation. There are 216 possible 16-bitblocks 0000000000000000, 1111111111111111. Each operation with the set of possible 16-bit blocks is an algebraic group. Bitwise XOR is bitwise addition modulo 2, and addition modulo 216 is the usual group operation. Some spin must be put on the elements – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 (i.e., 0000000000000000) is not an element of the multiplicative group.



In particular, the following requirements must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process:

1. Data aggregation is possible only if intermediate nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes that send data packets toward the base station must encrypt them with keys available to the aggregator nodes.

2. Data dissemination implies broadcasting of a message from the aggregator to its group members. If an aggregator shares a different key (set of keys) with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with a different key, in order
to broadcast a message to all of the nodes .But transmissions must be kept as low as possible because of their high-energy consumption rate.

3. Confidentiality: In order to protect sensed data and communication-changes between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network, case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station Hence ,confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information

4. Integrity and Authentication: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions.

https://dx.doi.org/10.22161/ijaers/3.10.11 *ISSN: 2349-6495(P) | 2456-1908(O)*

However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence, authentication mechanisms should be "collective" and aim at securing the entire network.

First, we focused on the establishment of trust relationship among wireless sensor nodes, and presented a key management protocol for sensor networks. The protocol includes support for establishing four types of keys per sensor node: individual keys shared with the base station, pairwise keys shared with individual neighboring nodes, cluster keys shared with a set of neighbors, and a group key shared with all the nodes in the network. We showed how the keys could be distributed so that the protocol can support in-network processing and efficient dissemination, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. Applying the protocol makes it hard for an adversary to disrupt the normal operation of the network.

In Hybrid Cryptosystem System, security is combination of more algorithm than base paper but still requires less time to Verify and process. While they are not present in the base paper. Hybrid Cryptosystem to enhance the security we use combination of algos

1) Idea algo.
2) MD5
3) ECB (ELECTRONIC CODE BOOK)
4) Hashing code

Comparative Result analysis

In my Base Paper we have used CP-ABE systems i.e. Cipher text-policy attribute-based encryption which is a promising cryptographic solution to the access control issues. While its communication Cost is higher than New Hybrid Cryptography Technique. Comparative results can see in Graph as:

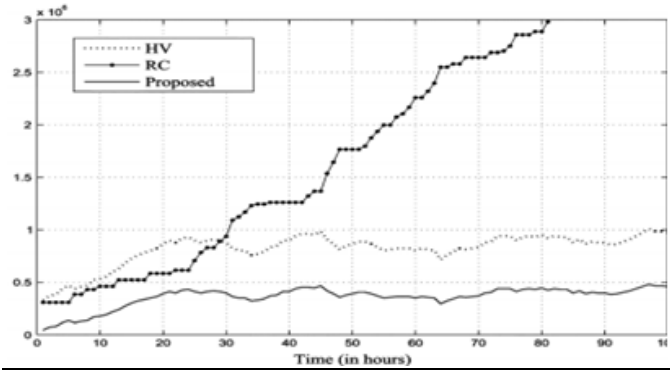


Fig.7.1: Communication cost in CP-ABE System

Number of conversion and verification time is more in base paper CP-ABE System then Hybrid Encryption by Using Idea Algorithm and MD5.

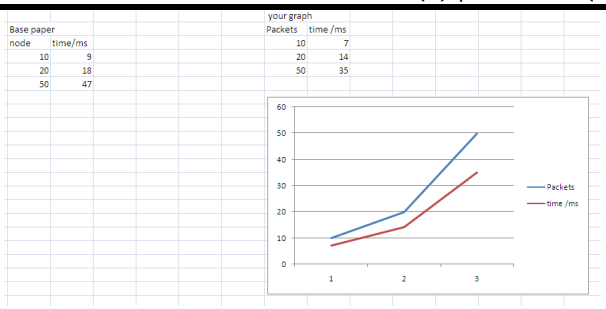


Fig 7.2 Packets Vs Time Graph

V. CONCULSION

The corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key in the cipher text are re-encrypted by the storage node with a random, and the cipher text components corresponding to the attributes are re-encrypted with the updated attribute group keys. Even if the user has stored the previous cipher text exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the pervious cipher text.

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 design for sparse ad hoc networks with mobile nodes," in *Proc. ACM MobiHoc, 2006, pp. 37–48.*

[4] S. Roy andM. 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] [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] [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.

https://dx.doi.org/10.22161/ijaers/3.10.11 *ISSN: 2349-6495(P) | 2456-1908(O)*

[9] D. Huang and M. Verma, "ASPE: Attribute-based secure policy enforcement n vehicular ad hoc networks," *Ad Hoc Netw.*,vol. 7, no. 8,pp. 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 attributebased encryption," in *Proc. IEEE Symp. Security Privacy*, 2007, pp. 321–334