Secure Communication in Decentralized Disruption Tolerant Military Networks Using CP-ABE and 2PC Protocol

[1]Nayanika Bhargava, [2]Sahil Bhasin, [3]J.Jeyasudha
[1,2]Student, [3]Assistant Professor
SRM University, Chennai.

Abstract **- In military networks, the network connections may be disconnected by jamming, environmental factors and mobility. Disruption-tolerant networks is a successful solution for communication between nodes in extreme environments and access the confidential information. The problem in the military environment such as hostile region or battlefield is intermittent connectivity and network partitions .Cipher Text policy-Attribute Based Encryption is the cryptographic solution for access control problems. There are so many challenges like attribute revocation, key escrow problem and coordination among attributes in applying CP-ABE in decentralized disruption tolerant networks. Here we propose a secure data retrieval using CP-ABE and 2 PC Protocol in decentralized disruption tolerant networks and multiple key authorities manage their attributes independently.**

Index Terms **- Disruption Tolerant Networks, Cipher Text Policy Attribute Based Encryption, Attribute Revocation, Key Escrow Problem, 2 PC Protocol**

I. INTRODUCTION

A secure data retrieval scheme using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently is used. It is demonstrated how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

Due to the disturbances and jamming of wireless connections in military areas between the soldiers and the commanders Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments [1]–[3]. 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. 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)].

Here we use Ciphertext-policy ABE (CP-ABE) and 2PC Protocol to provide 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.

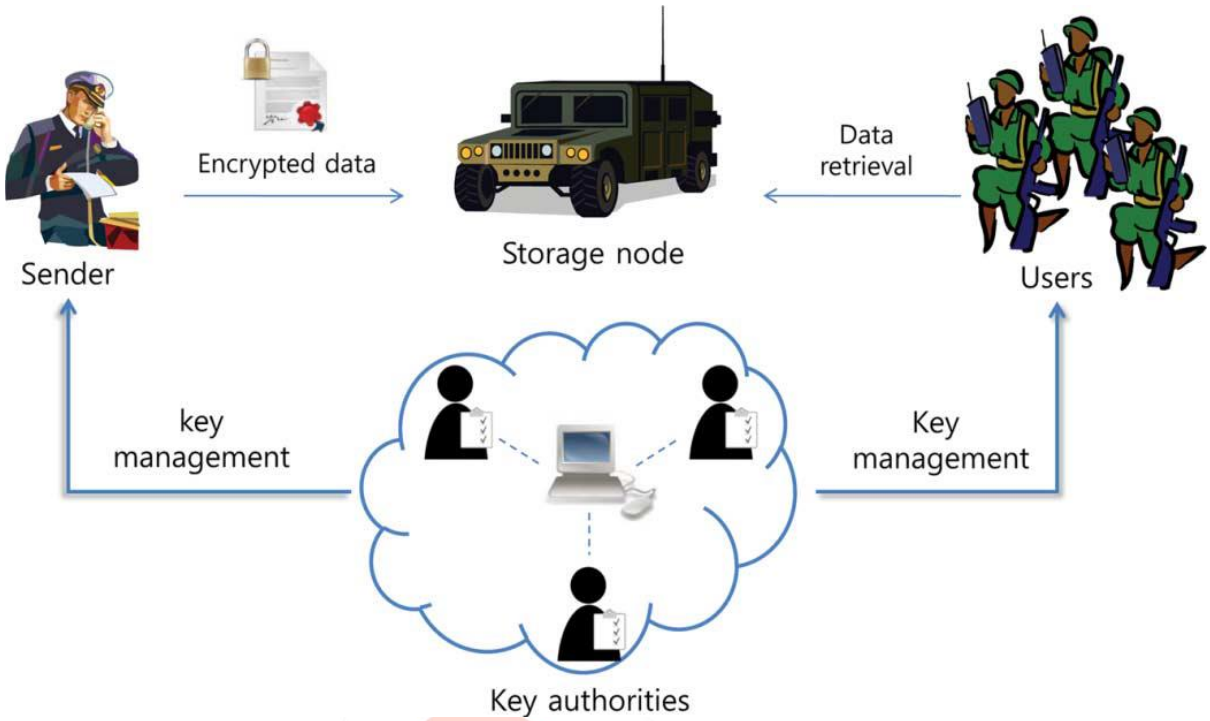

Figure 1 : System Architecture

II. DISRUPTION TOLERANT NETWORKS(DTN)

A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. There are several aspects to the effective design of a DTN, including:

1. The use of fault-tolerant methods and technologies.
2. The quality of graceful degradation under adverse conditions or extreme traffic loads.
3. The ability to prevent or quickly recover from electronic attacks.
4. Ability to function with minimal latency even when routes are ill-defined or unreliable.

Fault-tolerant systems are designed so that if a component fails or a network route becomes unusable, a backup component, procedure or route can immediately take its place without loss of service. At the software level, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems immediately. In hardware, fault tolerance is achieved by component and subsystem redundancy.

Graceful degradation has always been important in large networks. One of the original motivations for the development of the Internet by the Advanced Research Projects Agency (ARPA) of the U.S. government was the desire for a large-scale communications network that could resist massive physical as well as electronic attacks including global nuclear war. In graceful degradation, a network or system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative.

Electronic attacks on networks can take the form of viruses, worms, Trojans, spyware and other destructive programs or code. Other common schemes include denial of service attacks and malicious transmission of bulk e-mail or spam with the intent of overwhelming network servers. In some instances, malicious hackers commit acts of identity theft against individual subscribers or groups of subscribers in an attempt to discourage network use. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers can be provided with antivirus software and individual computers in the system can be protected by programs that detect and remove spyware.

As networks evolve and their usage levels vary, routes can change, sometimes within seconds. This can cause temporary propagation delays and unacceptable latency. In some cases, data transmission is blocked altogether. Internet users may notice this as periods during which some Web sites take a long time to download or do not appear at all. In a DTN, the frequency of events of this sort is kept to a minimum.

III. CIPHER TEXT POLICY- ATTRIBUTE BASED ENCRYPTION

In ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a ciphertext specifies an access policy over a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the respective ciphertext. Policies may be defined over attributes using conjunctions, disjunctions and(k,n)-threshold gates, i.e., k out of n attributes have to be present (there may also be non-monotone access policies with additional negations and meanwhile there are also constructions for policies defined as arbitrary circuits). For instance, let us assume that the universe of attributes is defined to be {A,B,C,D} and user 1 receives a key to attributes {A,B} and user 2 to attribute {D}. If a ciphertext is encrypted with respect to the policy (A∧C)∨D, then user 2 will be able to decrypt, while user 1 will not be able to decrypt.

CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people

who satisfy the associated policy can decrypt data. Another nice features is, that users can obtain their private keys after data has been encrypted with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows to decrypt. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data.

Key-Policy ABE

KP-ABE is the dual to CP-ABE in the sense that an access policy is encoded into the users secret key, e.g., (A∧C)∨D, and a ciphertext is computed with respect to a set of attributes, e.g., {A,B}. In this example the user would not be able to decrypt the ciphertext but would for instance be able to decrypt a ciphertext with respect to {A,C}.

An important property which has to be achieved by both, CP- and KP-ABE is called collusion resistance. This basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a ciphertext that neither of them could decrypt on their own (which is achieved by independently randomizing users' secret keys).

Beyond ABE

ABE is just one type of the more general concept of functional encryption (FE) covering IBE, ABE and many other concepts such as inner product or hidden vector encryption (yielding e.g., searchable encryption) etc. It is a very active and young field of research and has many interesting applications (in particular in the field of cloud computing).

III. ATTRIBUTE REVOCATION

Revocation is a vital open problem in almost every crypto system dealing with malicious behaviors. In cipher text policy attribute based encryption, unlike traditional public key cryptosystem, different users may hold the same functional secret keys related with the same attribute set leading to additional difficulties in designing revocation mechanism. we propose the cipher text policy attribute based encryption scheme with efficient revocation which can be proved secure in the standard model Their solutions are to append to each attribute an expiration date (or time) and distribute a new set of keys to valid users after the expiration. The periodic attribute revocable ABE schemes have two main problems

The first problem is the security degradation in terms of the backward and forward secrecy. For example, 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 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 reencrypted with the newly updated attribute keys by periodic rekeying (backward secrecy).

In cryptography, forward secrecy is a property of key- protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. The key used to protect transmission of data must not be used to derive any additional keys, and if the key used to protect transmission of data is derived from some other keying material, then that material must not be used to derive any more keys. In this way, compromise of a single key permits access only to data protected by that single key.

The other is the scalability problem. Scalability is the ability of a system, network, or process to handle a growing amount of work in a capable manner or its ability to be enlarged to accommodate that growth it can refer to the capability of a system to increase its total output under an increased load when resources (typically hardware) are added. An analogous meaning is implied when the word is used in an economic context, where scalability of a company implies that the underlying business model offers the potential for economic growth within the company.

Scalability, as a property of systems, is generally difficult to define[2] and in any particular case it is necessary to define the specific requirements for scalability on those dimensions that are deemed important. It is a highly significant issue in electronics systems, databases, routers, and networking. A system whose performance improves after adding hardware, proportionally to the capacity added, is said to be a scalable system

IV. KEY ESCROW PROBLEM

Key Escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys Under normal circumstances, the key is not released to someone other than the sender or receiver without proper authorization. Key escrow systems can be considered a security risk at the user puts access to information into the hands of the escrow agent holding the cryptographic key; however, key escrow systems are used to ensure that there is a backup of the cryptographic key in case the parties with access to key lose the data through a disaster or malicious intent.

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. Thus, the key escrow problem is inherent such that the key authority can decrypt every ciphertext addressed to users in the system by generating their secret keys at any time

V. 2 PC PROTOCOL

In transaction processing, databases, and computer networking, the two-phase commit protocol (2PC) is a type of atomic commitment protocol (ACP). It is a distributed algorithm that coordinates all the processes that participate in a distributed atomic transaction on whether to *commit* or *abort* (*roll back*) the transaction (it is a specialized type of consensus protocol). The protocol achieves its goal even in many cases of temporary system failure (involving either process, network node, communication, etc. failures), and is thus widely utilized. However, it is not resilient to all possible failure configurations, and in rare cases user (e.g., a system's administrator) intervention is needed to remedy an outcome. To accommodate recovery from failure (automatic in most

cases) the protocol's participants use logging of the protocol's states. Log records, which are typically slow to generate but survive failures, are used by the protocol's recovery procedures. Many protocol variants exist that primarily differ in logging strategies and recovery mechanisms.

In this system, key authorities are the key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. Storage node is an entity that stores data from senders and provide corresponding access to users. Sender stores the confidential information in the external data storage for ease of sharing. Sender is responsible for defining access policies and encrypt the messages and store it in the storage node. User is the mobile node who wants to access the data stored in the storage node. Since key authorities are less trusted so 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.

VI. EXISTING SYSTEM

In the existing system, they use distributed KP-ABE scheme that solves the key escrow problem in a multi authority system. In this system all (disjoint) attribute authorities are participating in the key generation protocol in a distributed way. In the existing system , it proposed a decentralized approach using ABE in the multi authority network environment. Here it achieved the combined access policy over the attributes issued from different authorities The major problem is security degradation in terms of forward and backward secrecy. Another thing is scalability problem. Because of the fully distributed approach, it faces the performance degradation. In the decentralized approach in faces the problem of efficiency and expressiveness of access policy. by simply encrypting data multiple times.

In the context of KP- 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.

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 nonrevoked users can update their keys. This results in the "1-affects- N" problem, which means that the update of a single attribute affects the whole nonrevoked users who share the attribute [19]. This could be a bottleneck for both the key authority and all nonrevoked users.

VII. PROPOSED SYSTEM

Here we propose a attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. In this system, key authorities are the key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities Storage node is an entity that stores data from senders and provide corresponding access to users. Sender stores the confidential information in the external data storage for ease of sharing. Sender is responsible for defining access policies and encrypt the messages and store it in the storage node. User is the mobile node who wants to access the data stored in the storage node. Since key authorities are less trusted so 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.

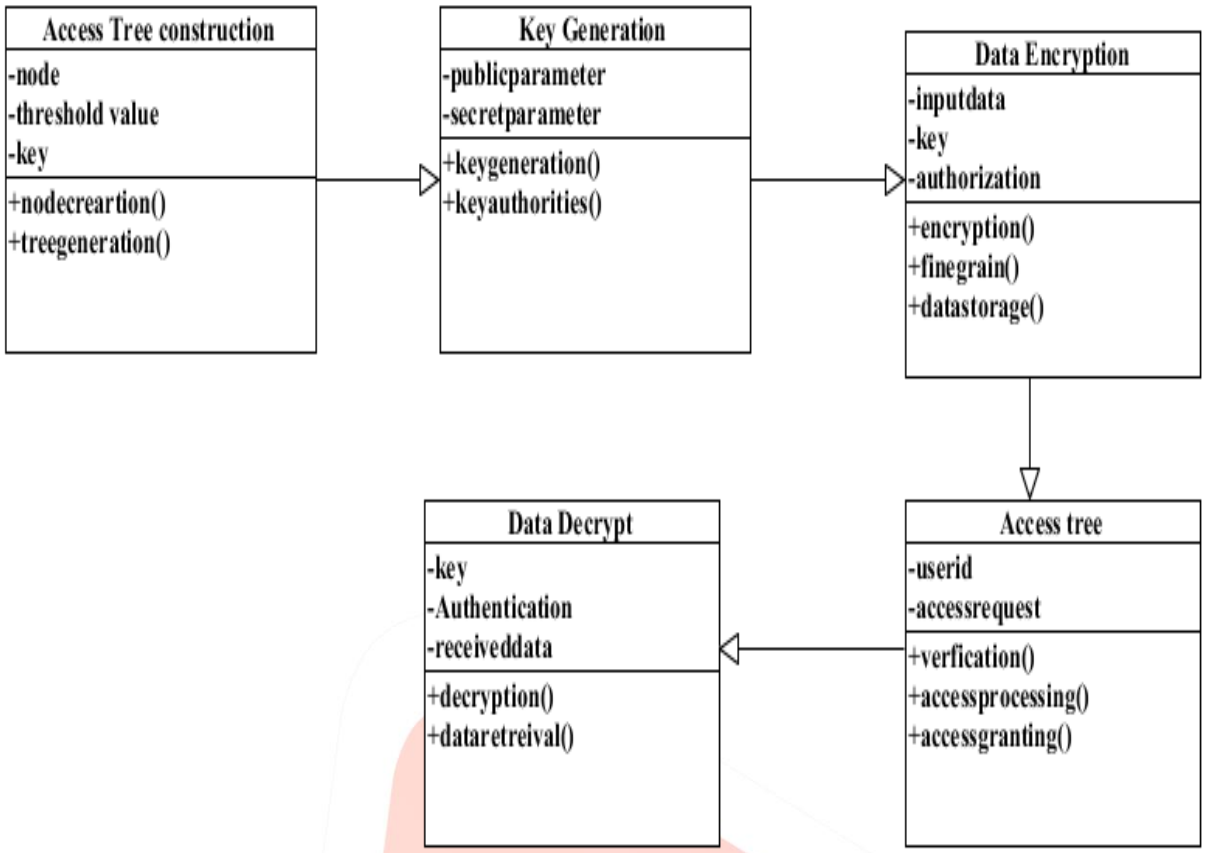

Figure 2 : Class Diagram for the proposed system

Secure data retrieval decentralized DTN enhancing CP-ABE Improving efficiency and performance of the system by solving key escrow and backward secrecy problems. It is securing the network system It can be used for

1. Dynamic communications for emergency/rescue operations.
2. Military network communication application
3. Disaster relief efforts

VIII. CONCLUSION

Disruption Tolerant network is a successful solution in military applications. In military networks, the user acces the confidential information which is exploits in the external storage node. Here we proposed an efficient and secure data retrieval method using CP-ABE for decentralized DTNs where multiple key authorities manage their attributes independently. The fine-grained key revocation can be done for each attribute group. 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. 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] 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 schemefor disruption tolerant networks," inProc. IEEE MILCOM, 2006, pp.1–6.

[3] M.M.B.Tariq,M.Ammar,andE.Zequra,"Message ferry route design 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 cipher text policy attribute-based encryption (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.