SECURED DECENTRALIZED CONFIDENTIAL DATA DISTRIBUTED ACROSS A DISRUPTION-TOLERANT MILITARY NETWORK. WITH THE ALGORITHM MD5 AND 3DES

RHATAVAL AVADHUT DHONDIRAM
ME E&TC BVCOE Kolhapur
E-mail: avadhut.rhataval@gmail.com

PROF.DR.K.R.DESAI
Guide, Department of E&TC
Bharati Vidyapeeth College of Engineering, Kolhapur.

ABSTRACT

Confidential information or data reliably through the operation of external storage nodes. Some of the most difficult problems in this scenario are the application of approval policies and updating the policies for secure data recovery. The attribute-based encryption of cipher text policy is a promising cryptographic solution for access control issues. However, the problem of using CP -ABE in the decentralized tolerance network poses some challenges of security and privacy in terms of the revocation of attributes, the blocking of keys and the coordination of attributes of different authorities. We propose a secure scheme of data rescue, by using the idea of decentralized, tolerant networks in which multiple key management administrators independently manage their attributes. We show how to use the proposed mechanism to safely and effectively manage confidential information or data distributed in the gust of the military network.

KEYWORDS: Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN).

INTRODUCTION

Mobile units in a military environment, such as a battlefield or a hostile region, may suffer from intermittent disconnection of the network and frequent partitions. Disruption-tolerant network (DTN) technologies are successful solutions that allow wireless devices that soldiers can communicate in this extreme network environment when there is no end-to-end connection between the source and target pairs, messages from the source node. It would be necessary to wait in intermediate nodes for a significant period of time until the connection is established. Data storage or duplication of DTN, so only authorized mobile nodes can quickly or efficiently receive or receive the necessary information. Many military applications require enhanced protection of sensitive data, including cryptographically compulsory access control methods and a differentiated access service. For example, specify data access policies that are defined according to user attributes or roles that are managed by key authorities.

DTN NETWORK ARCHITECTURE

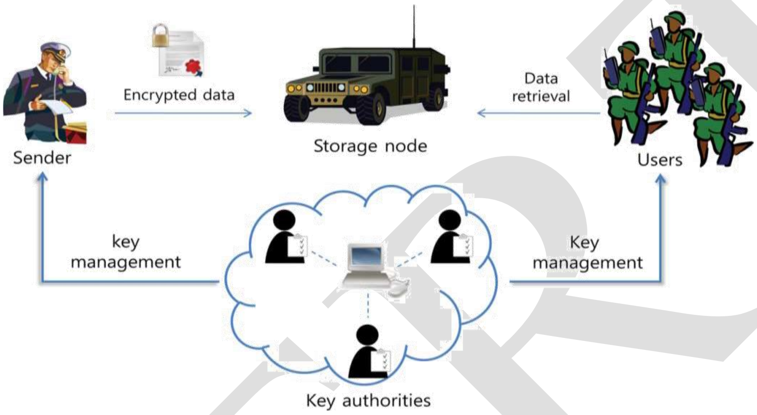
1) KEY AUTHORITIES: These are key generation centers that generate public/secret parameters for CP-ABE. The main authorities consist of a central government and several local authorities. We assume that there are reliable and reliable communication paths between the Central Authority and each municipality in the initial phase of the building and the creation of the key. Each local authority administers various attributes and provides the user with corresponding attribute keys. They grant different user access based on user attributes. Mainly think honest, but curious. That is, they will perform honestly transferred tasks in the system; However, they want to know as much as possible information about encrypted content.

2) STORAGE NODE: This node stores data from senders and provides appropriate access to users. It can be mobile or static, we also assume that the storage node is half-protective, which is honest, but curious.
3) Sender: This node has confidential messages or data (such as the commander) and wants to store it in an external storage node for easy exchange or reliable delivery to users in extreme network environments. The sender is responsible for defining an access policy based on the attribute and encrypting its own data by encrypting the data according to the policy before storing it on the storage node.

4) USER: This mobile user wants to access data stored on storage nodes (for example, soldiers). If a user has a set of attributes that correspond to an access policy for data encrypted by the sender, then he can decrypt the IDEAL ALGORITHM and get the data.

Because the key message information is semi-secure, they should be kept from accessing the open data text in the storage node. At the same time, they should be able to assign keys to users. In order to implement this controversial request, the Central Authority and local authorities participate in the 2PC Arithmetic Agreement with a secret key and provide stand-alone key components for users in the key issue. Protocol 2PC does not allow them to learn the main secrets of each other so that none of them could generate the entire set private key of users separately. So we start from the assumption that the central government does not collide with the local authorities (otherwise they can guess the secret keys of each user and share their main secrets).

SYSTEM FLOW



MOTOVATION

We offer a multimedia scheme CP ABE for secure data retrieval in decentralized DTNs. The attribute-based encryption (ABE) concept is a forward-looking approach that meets the prerequisites for secure data retrieval in the DTN. ABE has a mechanism that allows you to control access to encrypted data about access policies and attributes associated with the private and encrypted text. In particular, the ABE (CP-ABE) policy of encrypted text provides a scalable way of encrypting data, thereby encrypting or defining a set of attributes that the decrypt or must have to decrypt the encrypted text. Each local authority provides users with partial personalization and attributes of key components and performs a secure 2PC agreement with the central authority. The key attributes of each user can be updated individually and immediately.

The main priority for solving the following problems in the proposed project is:

1. Key transactions
2. Decentralized ABE scheme
3. Decentralized ABE scheme
4. Central authority and local authorities are engaged in MD5 Also, which prevents them from knowing each other.
5. The user does not have to revoke his attributes and execute access policies
6. The sender is responsible for maintaining the access system

PROBLEM DEFINITION

1) CONFIDENTIALITY OF DATA. Unauthorized users who do not have sufficient credentials corresponding to the access policy should avoid access to normal data in the storage node. In addition, unauthorized access from the storage node or key authorities should also be prevented.

2) CONSISTENCY: When multiple users converge, they can decrypt the encrypted text by combining their attributes, even if each user can not only decrypt an encrypted text [11] - [13]. Suppose there is a user with attributes {"Battalion 1", "Region 1"} and another user with the attributes {"Battalion 2", "Region 2"}. They are able to encrypt the encrypted text according to access policy ("Battalion 1" and "Region 2"), even if each of them cannot decrypt it separately. We do not want these colluders to decrypt confidential information by combining their attributes. We also consider an attack of collusion between curious local authorities to get the keys of the users.

3) BACKWARD AND FORWARD SECRECY: In the ABE context, confidentiality means that any user with attributes cannot access the normal text of previous data until an attribute is received. On the other hand, the perspective meaning means that any user who falls on the attribute can't access the open text of subsequent data after it has deleted the attribute unless other valid attributes it has an access policy.

4) KEY ESCROW: In the CP-ABE, the key management authority generates a private user key and applies the most important secret authorization key to the associated attribute set. Thus, the key body can decrypt any encrypted text addressed to particular users by generating its attribute keys. If the key authority is hacked by opponents when used in hostile environments, this can be a potential threat to the privacy of data or confidentiality, especially if the data is very sensitive. Key deposition is an inherent problem also in systems with multiple authorities, if each key authority has the entire privilege to create its own attribute keys with its own.

OBJECTIVE

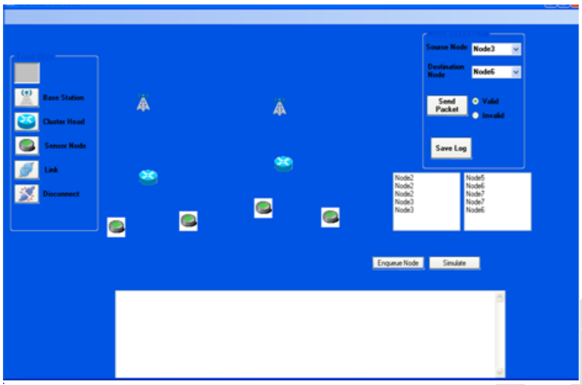
1) To achieve this somewhat controversial demand, the central government and local authorities intervene in the arithmetic MD5 algorithm with their own secret keys and highlight the key components regardless of the key phase of withdrawal.
2) Algorithm MD5 does not allow them to learn the main secrets of each other, so none of them can generate the entire set of private keys of users individually
3) We offer a security-based security data retrieval system in context with CP-ABE for decentralized DTN. The proposed program achieves the following results. First, immediate rollback of attributes increases the delay of data in the reverse / forward direction, reducing the windows of vulnerabilities.
4) Secondly, ciphers can define a fine-grained access policy using a monotonous access structure by attributes issued by any selected set of credentials. Third, a keyless protocol that uses the properties of a decentralized DTN architecture triggers a key issue with depositing.
5) The key output protocol generates and outputs a user key by executing a secure two-way calculation protocol (2PC) between the primary permissions with its own master secrets. The 2PC protocol forces the key authorities to receive any secret sensitive information from each other so that neither of them can generate the entire set of user keys.

METHODLOGY

We provide an attribute-based schema for the search for protected data using CP ABE for remote DTNs. The proposed system has the following benefits: Firstly, immediate resetting of attributes increases the confidentiality of sensitive data in the opposite direction and forward, causing weaknesses. Secondly, digits can define a fine-grained access policy by using a monotonous access structure by attributes issued by any selected set of credentials. Thirdly, the key deposition problem is solved by a keyless deposition protocol that uses the features of a decentralized DTN architecture.
The key issue log generates and outputs the user's secret key by running a secure two-party protocol (2PC) among the key authorities with their own main secrets. The 2PC protocol pushes key bodies away from receiving sensitive information from each other so that none of them can generate the entire set of user keys. Thus, users do not have to fully trust the authorities to protect their data for sharing. The confidentiality of the data and the confidentiality can be applied cryptographically against any curious key elements or storage nodes in the proposed regulation.

3 DES with MD5 ALGORTHIM

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. Thereare216possible16-bitblocks: 0000000000000000, 1111111111111111. Each process with a set of possible 16-bit blocks is an algebraic group. The bitwise bit XOR is a bitwise addition module 2 and is the normal group operation. Some spin must be put on the components – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 (i.e., 0000000000000000) is not an component of the multiplicative group.



Source Node: Node3
Destination Node: Node6
● Valid
○ Invalid

Node2
Node2
Node2
Node3
Node3

Node5
Node6
Node7
Node7
Node6

CONFIDENTIALITY: To protect sensitive data and exchange data between sensory nodes, it is important to ensure the privacy of messages. In the sensor network, the case, which is generally achieved by asymmetric cryptography as asymmetric or public-key cryptography, is generally regarded as too expensive. Despite the fact that encryption protects against external attacks, it does not protect against attack compromises because an attacker can use the recovered cryptographic key material to successfully listen, imitate, or participate in a secret network connection. In addition, although the confidentiality guarantees the security of communication within the network, it does not prevent the misuse of information to come to the base station. Therefore, the confidentiality must also be combined with the right management policies so that only authorized users can have access to sensitive information.

INTEGRITY AND AUTHENTICATION: Integrity and authentication are required for activation at sensor nodes to detect modified, injected or reproduced packets. Although it is clear that critical applications need authentication, it's reasonable to use them for other applications; otherwise the owner of the sensor network can get the wrong image of the perceived world and take inappropriate solutions. However, authentication itself does not solve the problem of node migration, since compromised nodes can still be authenticated on the network. Therefore, authentication mechanisms should be "collective" and aimed at ensuring the security of the entire network.

- In particular, a key management system should support the following requirements to facilitate the aggregation and dissemination of data process:
  1. Data aggregation is only possible if intermediate nodes have access to encrypted data so that they can extract measured values and apply aggregation functions. Therefore, the nodes that send data packets to the base station must encrypt them using keys that are available to the aggregator nodes.
  2. The dissemination of data implies the transmission of a message from the aggregator to members of its group. If the aggregator uses a different key (or set of keys) with each of the sensors within its group, then it must make multiple transmissions encrypted each time with a different key to send the message to all nodes but the transmissions must be kept as low as possible because of their high speed energy consumption
  3. Confidentiality: To protect the communication between sensitive data and sensor nodes, it is important to ensure the confidentiality of the message. In the sensor network, this is usually done using symmetric cryptography as an asymmetric or public encryption key, which is usually considered too costly. However, although encryption protection is protected from external attacks, this does not prevent internal attacks/nodes from being compromised, since an attacker can successfully use, simulate, or participate in a secret communication over the network using the recovered key encryption key material. In addition, although confidentiality ensures that security within the network cannot prevent abuse of information coming to the base station. Therefore, confidentiality should also be combined with a proper management strategy, so that only authorized users can access confidential information.

- Integrity and Authentication: Integrity and authentication are necessary to enable discovery of sensors, modified, injected or reproduced packets. Although it is clear that critical applications need authentication, it's reasonable to use them for other applications; otherwise, the owner of the sensor network can get the wrong image of the perceived world and take inappropriate solutions. However, authentication itself does not solve the problem of node migration, since compromised nodes can still be authenticated on the network. Therefore, authentication mechanisms should be "collective" and aimed at ensuring the security of the entire network.
- First, we focused on establishing the relationship of authentication between wireless sensor nodes and presented a key management protocol for sensor networks. The protocol supports the configuration of four types of keys on the sensor node: a separate key common to the base station, a shared key shared with each neighboring node, a cluster key shared with the neighboring set, and all nodes in the network key. We showed how you can distribute keys so that the protocol can support intranet processing and efficient distribution while limiting the impact of the node's vulnerability on the immediate network environment of the compromised node. The use of the protocol makes it difficult for the opponent to disrupt the normal operation of the network.

MODULES:

1. Development of a packet encryption module. In this module, we will connect the network. Each node is connected to an adjacent node and is used independently in the network area and also unfolds every port number at the node. Intrusion Detection is defined as a mechanism for a packet in the network to detect the presence of inappropriate, abnormal, or abnormal roaming attackers. In this module, check whether the path is activated or not. If the path is activated, the packet is sent to the actual destination. Otherwise, the package will be deleted. In accordance with the port not only, we will find the route authorized or unauthorized.
2. Developing Software Module. In this module, you can search and select the source file. And the selected data is converted into a fixed packet size. And the package is sent from the source to the destination.

CONCULSION

These technologies are becoming successful solutions in military applications, allowing wireless devices to communicate with each other and reliably use confidential information using external storage nodes. This is an extensible encryption solution for access control and data protection. In this paper, we proposed an efficient and safe method of extracting data using this method for decentralized DTNs, where several key bodies independently manage their attributes. The problem of an integral key deposit is solved so that the confidentiality of the stored data is also guaranteed in an aggressive environment in which the most important bodies can be compromised or not fully trusted.

REFERENCES

I. 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.*

II. M. Chuah and P. Yang, “Node density-based adaptive routing scheme for disruption tolerant networks,” in *Proc. IEEE MILCOM, 2006, pp.*1–6.

III. M. M. B. Tariq, M. Ammar, and E. Zequra, “Message ferry route design for sparse ad hoc networks with mobile nodes,” in *Proc. ACM MobiHoc, 2006, pp. 37–48.*

IV. 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.

V. M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for DTNs,” in *Proc. IEEE MILCOM,* 2007, pp. 1–7.

VI. 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.*

VII. 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.

VIII. 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.

IX. 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.

X. Lewko and B. Waters, "Decentralizing attribute-based encryption," Cryptology ePrint Archive: Rep. 2010/351, 2010.

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