Research Paper

Volume : 4 | Issue : 5 | May 2015 • ISSN No 2277 - 8179

Efficient and Secure Data Retrieval for Military Networks

Engineering

KEYWORDS : Dynamic Source Routing (DSR), Digital Signature Algorithm(DSA),Secure data retrieval.

Pravia V M.Tech CSE, AWH Engineering College, Calicut, India

ABSTRACT

The military network environment consists of several mobile nodes. The main problem with such network is that intermittent connection, to avoid this problem military network use Disruption Tolerant Network (DTN). The most challenging issue in the military network is that secure retrieval of confidential data. Cryptographic solutions used to avoid this problem. Existing system uses Ciphertext–Policy Attribute Based Encryption (CP-ABE). In CP-ABE which use a storage node. The main function of storage node is that which can store the encrypted messages from the sender and provide these messages to the intended recipient. Problem with this scheme is that the storage node is semi trusted, any issue in the storage node may course loss of all data. To avoid these problems introduce a new scheme in which we can use routing for sending encrypted messages from sender to receiver instead of storing data in the storage node.

Introduction

Disruption Tolerant Network (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may be lack continuous network connectivity. Disruption may occur because of the limit of wireless radio range of mobile nodes.

Security concern for DTNs varies depending on the environment and application, though authentication and privacy are crucial. These security guarantees are difficult to establish in a network without persistent connectivity. The solution for this problem is that use of ad hoc network and distributed security research such as use of distributed security certificate authorities. Original solution from DTN include

- Use of encryption.
- The use of tamper evident table with gossiping protocol.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, generating ciphertext that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required. An authorized recipient can easily decrypt the message with the key provided by the originator to recipients, but not to unauthorized interceptors.

In the case of military network use Ciphertext–Policy Attribute Based Encryption (CP-ABE). Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

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.

In CP-ABE which use a storage node. The main function of storage node is that which can store the encrypted messages from the sender and provide these messages to the intended recipient. Problem with this scheme is that the storage node is semi trusted, any issue in the storage node may course loss of all data. To avoid these problems introduce a new scheme in which we can use routing for sending encrypted messages from sender to receiver instead of storing data in the storage node.

The routing scheme used in the new scheme is the dynamic routing. Dynamic routing, also called adaptive routing, describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid in response to the change.

RELATED WORKS

For the secure retrieval of confidential data in military networks we use different types of encryption schemes. Attribute Based Encryption (ABE)[1] is the most commonly used encryption method. In ABE the encryptor label each cipher text with a set of descriptive attributes. Each private key is associated with an access structure. The access structure used to identify which type of cipher text the key can decrypt. Each user's key is associated with a tree- access structure where the leaves are associated with attributes. If the attribute associated with a cipher text satisfy the key's access structure then the user will able to decrypt that specific cipher text.

Different encryption schemes are derived from ABE, they are Dynamic ABE[2][3],Cipher Policy-ABE(CP-ABE)[4], Bounded CP-ABE[5], Mediated CP-ABE[6] and Multi authority ABE[7].

In dynamic ABE, the ABE adds expiration timer to revoke private keys. After that expiration time the user cannot hold the attributes initially they have.

In CP-ABE scheme each user is associated with a set of attrib-

utes. The private key is generated based on the attribute set. The encryptor encrypts a message M used with an access structure which is expressed in terms of a set of selected attributes for M. the decryptor can decrypt the message if and only if their attribute satisfies the access structure used to encrypt the message M. Unauthorized users are not able to decrypt the ciphertext even if they collude.

Bounded CP-ABE can support access structure which can be represented by a bounded size access tree. The access tree has the threshold gate as its nodes. At the time of system setup it can choose the bounded size of access trees. The access tree is represented as tuple (d, num) where d is the maximum depth of access tree and num represents the maximum number of children each non leaf node might have. The encryptor selects the access tree that satisfying the upper bound.

Attribute revocation in CP – ABE is called Mediated CP-ABE. In this scheme the secret key is divided into two parts, one part for the mediator and other part for the user. For decrypting the message the user can contact with the mediator for getting the decryption token. The mediator keeps an attribute revocation list (ARL) and refuses to issue the decryption token for revoked attributes.

existing system

In the case of military networks the nodes are mobile because of this reason the network is suffer from intermittent connectivity and frequent partitions. To avoid this problem introduce a new type of network known as Disruption Tolerant Network (DTN). The most challenging issue for this scenario is that the enforcement of authorization policies and the policies update for secure data retrieval. The CP-ABE [8] is the most promising solution. In the case of decentralized DTNs CP-ABE[9][10] uses multiple key authorities to manage their attributes independently.

In CP-ABE it 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. Different users are allowed to decrypt different piece of data per the security policy.

Network Architecture

In this section we describe the network architecture of existing system

Fig 1. Architecture of secure data retrieval in a disruption-tolerant military network.

The network architecture consists of four entities they are

- Key Authorities: The entity used for the generation of both public and private key for CP-ABE. It consists of a central authority and several local authorities. There present a secure communication channel between central authority and local authorities. The main purpose of local authorities is that it manages different attributes and provides corresponding attribute keys to users
- Storage node: Storage node stores data from the senders and provides corresponding access structure to the users. Storage nodes may be mobile or static.
- Sender: The sender having confidential data and encrypt the message with particular access structure. After encrypting the message sender can store the data into the storage node. The last entity is the user. The user is a mobile node access data from the storage node.
- User: The user having a set of attributes and they can satisfy the access policy described by the sender. The user can decrypt the message if and only if they satisfy the access structure used by the sender for encrypting the message.

proposed system

In the case of military networks secure retrieval of confidential data is very important. For this purpose we use encryption techniques. The existing system uses cipher policy- attribute based encryption for data security. The main characteristic of existing system is that it uses a storage node. The administrator can encrypt message and store it into the storage node, and the recipient node can take the message from storage node and decrypt with corresponding attribute set. Storage node may static or dynamic. Problem with storage node is that once it may damage the entire data will be loss. To avoid this problem we propose a new scheme using dynamic routing. In the case of dynamic routing the data can be sending from administrator to receiver by using shortest path.

Another problem with existing system is that it uses a separate key authority, which increases the overhead and time delay. That is for each encryption and decryption the user can request for key to key authority and the key authority responds by providing corresponding key. It increases the time delay for encrypting and decrypting messages. To avoid this problem we use Digital Signature Algorithm(DSA). In the case of DSA there is no need for a separate key authority, that is key is automatically generated with the message.

Digital Signature Algorithm (DSA)

1. DSA Key Generation

1.1 Parameter generation

- Choose an approved cryptographic hash function *H*.
- Decide on a key length L and N. L to be a multiple of 64 between 512 and 1024
- Choose an *N*-bit prime *q*
- Choose an *L*-bit prime modulus *p* such that *p*–1 is a multiple of *q*.
- Choose *g*, a number whose multiplicative order modulo *p* is *q*.

The algorithm parameters (*p*, *q*, *g*) may be shared between different users of the system.

1.2 Per-user keys

- Given a set of parameters, the second phase computes private and public keys for a single user.
- Choose *x* by some random method, where $0 < x < q$.
- Calculate $y = g^x \bmod p$.
- Public key is (*p*, *q*, *g*, *y*). Private Key is *x*.

2. Signing

Let H be the hashing function and M be the message:

- Generate a random per-message value k where $0 < k < q$.
- Calculate $r = (g^k \pmod p) \pmod q$
- In the unlikely case that r=0, start again with a different random k.
- Calculate $s = k^{-1}(H(M)+xr) \pmod q$

- In the unlikely case that s=0, start again with a different random k.
- The signature is (r,s).

2. Verifying

- Reject the signature if 0<r<q or 0<s<q is not satisfied.
- Calculate $w = s^{-1} (\text{mod } q)$
- Calculate u1= H(M).w mod q
- Calculate u2= r.w(mod q)
- Calculate $v= ((g^{u1}y^{u2}) \text{mod } p) \text{mod } q$
- The signature is valid if v=r

Dynamic Source Routing (DSR)

1. Route discovery

- Check the unique ID of RREQ, if it is already received: discard RREQ

- Check the destination of RREQ, if it is the desired destination then send a route reply (RREP) to the source.
- Otherwise broad casts the RREQ message to its neighbors and also attach its own ID to the RREQ message.

2. Route maintenance

when source is using a discovered route to destination, source may detect that the route is broken. In such cases source may use an alternate route to the destination or start another route discovery phase to destination.

Network Architecture

In this section we describe the network architecture of proposed system

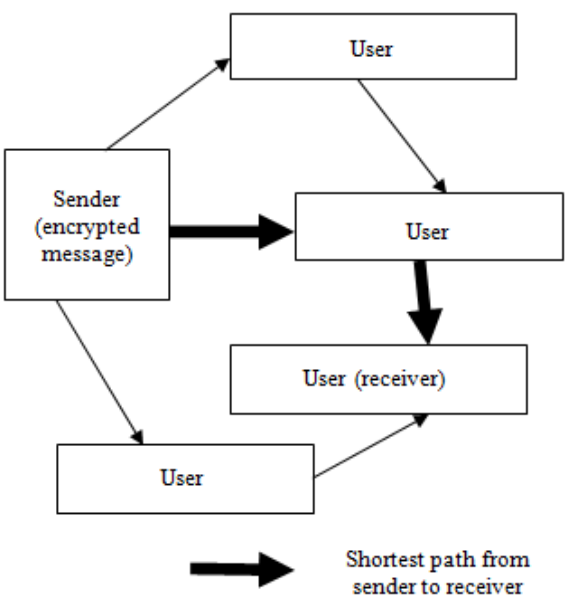

Fig 2. Architecture of secure data retrieval in proposed scheme.

The network architecture include 2 entities, they are

1) Sender: Having confidential data. It encrypts the message and sends to the user by using dynamic source routing algorithm.
2) User: User is the mobile node who wants to access encrypted message from the sender. Only the user that can specify by the sender can decrypt the message.

Conclusion

In military networks all nodes are mobile. So they use wireless devices to communicate with each other. When a node want to send confidential message to another node it uses several security methods. The digital signature algorithm is the scalable cryptographic solution for the secure retrieval of confidential data. And the other problem is that how to send encrypted message from sender to indented recipient. For this we use dynamic source routing (DSR). In DSR the sender sends message to user by using shortest path, so the delay between sending a message and receiving the corresponding message is decreasing.

REFERENCE

[1] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. | [2] A. Lewko and B. Waters, "Decentralizing attribute-based encryption, "Cryptology ePrint Archive: Rep. 2010/351, 2010. | [3] 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. | [4] S. Roy andM. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," LehighCSE Tech. Rep., 2009. | [5] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption," in Proc. ICALP, 2008, pp.579–591. | [6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application, "in Proc. WISA, 2009, LNCS5932,pp.309–323. | [7] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in Proc. ACM Conf. Comput.Commun. Security, 2009, pp. 121–130. | [8] Junbeom Hur and Kyungtae Kang,"Secure data retrieval for decentralized disruption-tolerant military networks",IEEE transactions on networking vol:22,year 2014. | [9] 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. | [10] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proc. ACM Conf. Comput. Commun. Security,2007,pp.456–465. | |