International Journal of Research in Advent Technology, Vol.4, No.4, April 2016
E-ISSN: 2321-9637
Available online at www.ijrat.org

Securing Military Data Using CP-ABE and Triple-DES With Multi-Authority System

Prof N D Sonawane[1], Ashutosh Kumar[2], Petkar Shreyas[3], Prasad Jat[4], Gururaj Shettigar[5]
Department of Computer Enginering[1, 2, 3, 4,5], PDEA,s College of Engineering Hadapsar[1, 2, 3, 4,5]
Email: petkar.shreyas34@gmail.com[1] , ak48252@gmail.com[2]

Abstract- Portable devices in different bases of military such as battlefield or hostile region. These are more likely to suffer from network connectivity problem and different partitions from main stations of military base. Sometimes it is impossible to connect to the battalions at higher altitudes. So now a days, Disruption-tolerant network (DTN) technologies are very successful solution to such problems. That allows portable devices to communicate with other battalions and from central authority also and access the confidential data from the database which are stored in the encrypted format. Some of the most difficult challenge in this is the enforcement of policies for authorization of data from the battalion side.

Cipher text-policy attribute-based (CP-ABE) encryption is a trusted algorithm to control the access of data from other parties and also used to encrypt data. But it also adds some security and privacy challenges with regard to the data revocation and coordination of attributes from different authorities. We also secure the data retrieval using CP-ABE and Triple-DES algorithm. Triple-DES is an algorithm which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Keying option reduces the effective key size to 112 bits. But, this option is susceptible to certain chosen-plaintext or known-plaintext attacks, and thus, it is designated by NIST to have only 80 bits of security.

Index Terms- Access control, Ciper-Text encryption (CP-ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

1. Introduction

In many military base connectivity scenarios, connections of portable devices carried by battalions can be temporarily have connectivity problem by jamming of network, environmental factors, and movement of battalion, especially when they operate in hostile regions. Disruption-tolerant network (DTN) technologies are now days become successful solutions that allow devices to communicate with other battalions and bases in this extreme networking connectivity environment. Typically, when there is no end-to-end connection between a source battalion and a destination battalion pair, then the messages from the source battalion may need to wait in the intermediate devices for an unknown amount of time until the connection would be eventually resumed. We provide a CP-ABE based encryption formula that provides fine-grained control on access on the data retrieval from database. In a CP-ABE encryption formula, each battalion is assigned with a set of attributes which is provided by the commander and based on which the battalion's private key is generated. Vital information is encrypted under an access policy such that only those battalions whose attributes match with the attributes assigned by the commander are able to decrypt the encrypted message. Our policy can provide not only fine-grained control access to each content object. Although data sending is a vital design issue for all such is connection to the network sparsely, the ability to access vital data rapidly from database is also an important feature that a DTN should have since the ultimate goal of having such a network is to allow portable devices to access data quickly and efficiently. For example, in a battlefield, battalion need to access information related to detailed geographical region, intelligent information about enemy locations and its position, new commands from the general/commander, weather information etc. In addition, a particular data item may be of useful to multiple battalions so it makes sense to replicate the data item to different battalions, and store it at multiple devices so that it can be accessed by other devices. This allows us to save battery usage, bandwidth consumption and the data item retrieval time from database. Such data caching also means that the source battalion of the data items need not know the identities of the devices. Disruption-tolerant networks (DTNs) attempt to route the network messages via intermittently connected devices in the network. Routing in such environments or network is difficult because nodes have little information about the state of the distributed network and transfer opportunities between nodes are of limited duration. In this, we propose a protocol for effective routing of DTN messages. MaxProp is based on giving priority to both the schedule of data transmitted to other nodes and the schedule of packets to be dropped. These priorities are based on the path likelihoods to peers according to historical data and also on several

complementary mechanisms, including acknowledgments, a head-start for new packets, and lists of previous intermediaries. Our evaluations show that MaxProp performs better than protocols that have access to an oracle that knows the schedule of meetings between peers. Our evaluations are based on 60 days of traces from a real DTN network we have deployed on 30 buses. Our network, called UMassDieselNet, serves a large geographic area between five colleges. We also evaluate MaxProp on simulated topologies and show it performs well in a wide variety of DTN environments.

2. EXISTING SYSTEM

Now days the security in military application is done through wireless communication .but there are number of security related issues raised up in data transmission. So to overcome that drawback programmer newly introduced the secure data retrieval from decentralized military network. Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks this is our existing system. In which they mainly introduced the key generation, data send in encrypted format and decrypted at the receiver end. In this existing system they are used Cipher text-policy attribute-based encryption (CP-ABE).
This system having mainly four components,

- Key Authorities
- Commander
- Data Storage Node
- Battalion

Here, in this existing system the Key Authorities generate the public key and encrypt data using that key and sends the encrypted data to the commander along with the public key and public key is also send to the battalions directly also. Now, the commander again encrypts data with its own generated private key and sends the encrypted data to the Data Storage Node. Now the Battalion deployed in different regions retrieves the encrypted data from the Data Storage Node and using that public key they decrypt the data into plain text and obey the commands from the base camps.

But, in the existing system it is not known that the data retrieval is requested from authorized battalion or some other unauthorized groups. Hence, this is the major drawback of this system which is overcome in the proposed system.

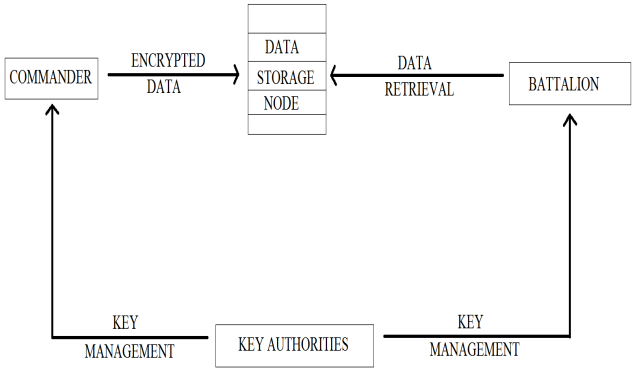

Fig 1 Existing System

2.1 Disadvantages

(1) Attribute Revocation: Key revocation mechanisms in CP ABE and KP-ABE, respectively. 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. It is a considerable scenario that users such as soldiers may change their attributes frequently,
The other is the scalability problem. The key authority periodically announces a key update material by uncast at each time-slot so that all of the non-revoked users can update their keys. This results in the "1-affects-" problem, which means that the update of a single attribute affects the whole non-revoked users who share the attribute. This could be a bottleneck for both the key authority and all non-revoked users.

(2) Key Escrow: 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.
3) Long range of Distance range communication must be difficult
4) Will not get high delivery ratio for messages with short deadline.
5) Additional transmission overhead is required in order to get the best delivery ratio.

3 PROPOSED SYSTEM

In this section, we provide a multi authority CP-ABE scheme with Triple-DES algorithm for secure data retrieval in decentralized DTNs. Each local authority

issues restricted personalized and attribute key components with Triple-DES encryption to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately more securely. Thus, the scalability and security can be enriched in the proposed scheme. There are total 11 steps where Commander sends message to the Battalion more securely.

1) The Key authority generates the public key and sends it to the Commander and the Battalion respectively.
2) After that the command from the commander is encrypted by the Triple DES key and the attributes are set. After that key is generated following attributes. This key and encrypted message is encrypted again and is stored to data node. The message is stored in the encrypted format on the storage node where the battalion will access the message from storage node directly.
3) The Battalion will request for the message to the storage node using the public key the storage node will give the response to the request as it will decrypt all the keys in order it has encrypted. After getting the response the battalion will generate key using ABE and decrypt the message using CP-ABE and also the Decrypt the same by Triple DES key.
4) Thus the following Fig indicates the total Flow of the proposed system in order to get the Command to the battalion securely.

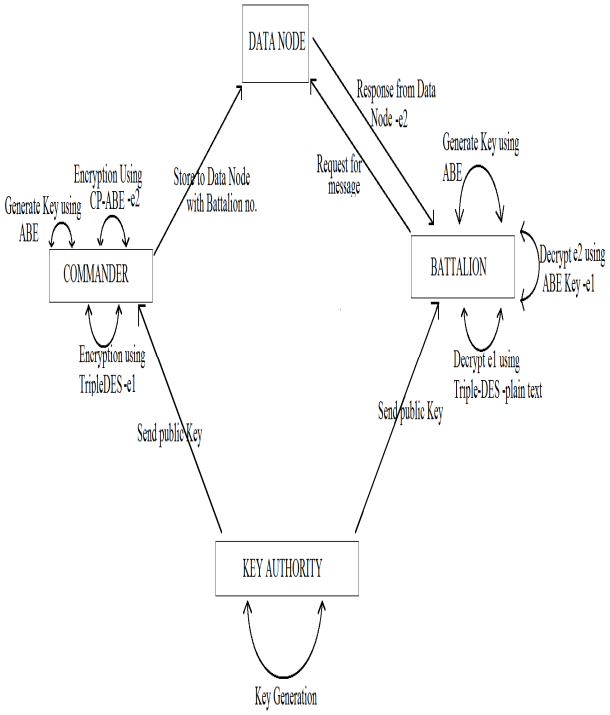

Fig 2 Proposed System

3.1 Triple-DES

In cryptography, **Triple DES** (**3DES**) is the common name for the **Triple Data Encryption Algorithm** (**TDEA** or **Triple DEA**) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

3.2 Algorithm:

Triple DES uses a "key bundle" that comprises three DES keys, K_1, K_2 and K_3, each of 56 bits (excluding parity bits). The encryption algorithm is:

$$\text{cipher text} = E_{K3}(D_{K2}(E_{K1}(\text{plaintext})))$$

i.e., DES encrypt with K_1, DES *decrypt* with K_2, then DES encrypt with K_3.

Decryption is the reverse:

$$\text{plaintext} = D_{K1}(E_{K2}(D_{K3}(\text{cipher text})))$$

I.e., decrypt with K_3, *encrypt* with K_2, then decrypt with K_1.

Each triple encryption encrypts one block of 64 bits of data.

In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

3.3 Advantages

1) Data Confidentiality: Illegal users who do not have enough approvals satisfying the access policy should be daunted from accessing the plain data in the storage node.
2) Collision: If multiple users collide they may be able to decrypt a cipher text by merging their attributes even if they cannot decrypt single-handedly.
3) Backward and Forward Secrecy**:** In the framework of ABE, backward secrecy means that any user who comes to hold an attribute should be prevented from accessing the plain text of previous data exchange before he holds the attribute.
4) Encryption can define a fine-grained access policy using any intonation access structure under attributes issued from any chosen set of authorities.
5) Battalion are not required to fully trust the authorities in order to protect their data to be stored.

4 CONCLUSION

The DTN technologies are becoming very useful solutions in military applications that allow wireless devices to communicate with other military bases in hostile regions and access the confidential vital information reliably by sending a retrieval message to external storage nodes. CP-ABE is a scalable encryption algorithm solution to the access control and secures data retrieval problems. In this paper, we proposed an efficient and secure data retrieval method using CP-ABE and Triple–DES for DTNs where multiple key authorities manage their attributes and public key independently and then send it to the commander and the battalions. The inherent key escrow problem is resolved such that the confidentiality of the stored data which is very important is guaranteed delivered to the battalion even under the hostile region where key authorities might be compromised or not fully trusted or cannot connect to the network. In addition, the fine-grained key revocation can be done for each attribute group to battalion assigned by the commander. 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] Junbeom hur and Kyungtae kang, *member, IEEE* "Secure data retrieval for decentralized disruption-tolerant military networks", IEEE transactions on networking, Vol: 22 no: 1 year 2014.

[2] 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.

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

[4] 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.

[5] 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.

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