Secure Data Retrieval for Military Networks

Snehal A. Patil
Guided By: Mrs Shital A. Patil

SSBT'S COET,Bambhori,Jalgaon

September 26, 2016

outline

1 Introduction

2 Public Key and Attribute

3 Key Point Attribute based Encryption

4 Working

5 System Description

6 Advantages

7 Disadvantages

8 Conclusion

9 References

10 Thanks

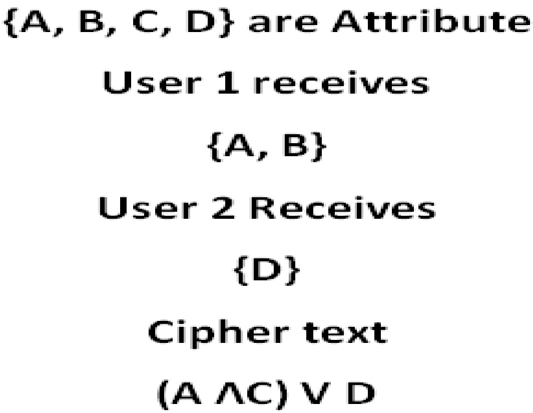
Introduction

- In many military network scenarios, connections of wireless devices carried by soldiers may be temporarily disconnected by jamming, environmental factors, and mobility, especially when they operate in hostile environments.
- *Disruption-tolerant network (DTN)* technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments.
- Many military applications require increased protection of confidential data including access control methods that are cryptographically enforced.

Public Key and Attribute

- Key Point Attribute based Encryption
- Ciphertext Policy Attribute based Encryption

Ciphertext Policy Attribute based Encryption



{A, B, C, D} are Attribute

User 1 receives

{A, B}

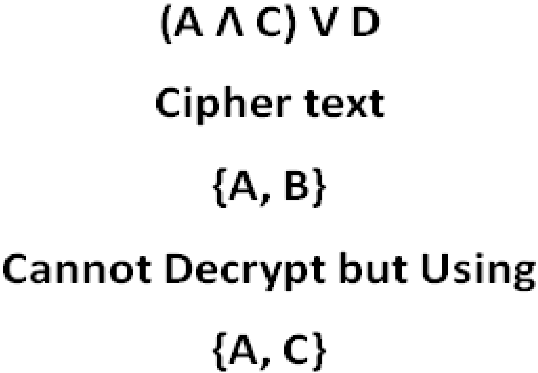
User 2 Receives

{D}

Cipher text

$(A \wedge C) \vee D$

Key point Attribute based Encryption



(A ∧ C) V D

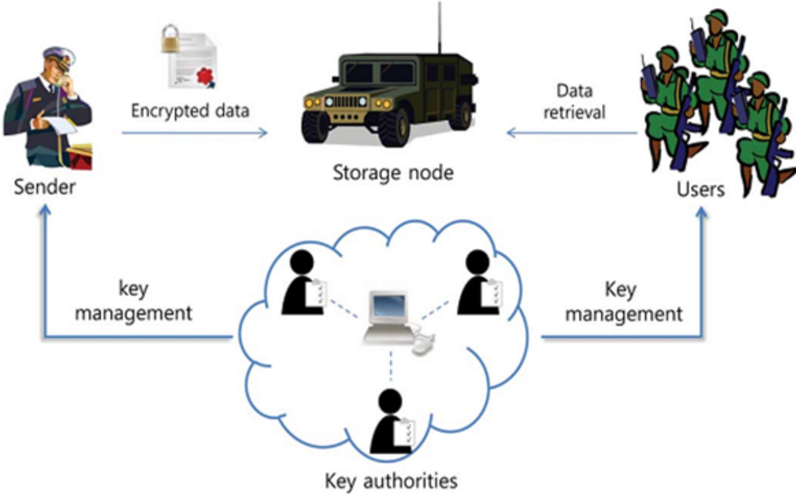
Cipher text

{A, B}

Cannot Decrypt but Using

{A, C}

Architecture of secure data retrieval for military network.



System Description

- Key Authorities: They are key generation centers that generate public/secret parameters for CPABE. The key authorities consist of a central authority and multiple local authorities.
- Storage node: This is an entity that stores data from senders and provide corresponding access to users.
- Sender: This is an entity who owns confidential messages or data and wishes to store them into the external data storage.
- User: This is a mobile node who wants to access the data stored at the storage node.

Advantages

- Data confidentiality
- Collusion-resistance:
- Backward and forward Secrecy:

Disadvantages

- the coordination of attributes issued from different authorities.
- the key escrow problem.Generate private keys of users and give athority to master key.
- The problem of applying the ABE to DTNs introduces several security and privacy challenges.

Conclusion

- Secure data retrival technologie is successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information.
- CP-ABE is a cryptographic solution to secure data retrieval issues.

References

- Secure Data Retrieval Using CPABE for Decentralized Disruption Tolerant Military Networks C. Rajeshwar Reddy 1, N.V. Sailaja
- Poon CCY, Bonato P: Wearable medical systems for p-Health. IEEE Reviews in Biomedical Engineering 2008
- Caudill TS, Lofgren R, Jennings CD, Karpf M: Commentary: Health care reform and primary care: training physicians for tomorrows challenges Acad Med 2011.

Thank You