

## “Secured Data Retrieval Disruption Tolerant Network”

Pushpraj Deshkar<sup>1\*</sup>, Amit Pampatwar<sup>2</sup>, Raana Syeda<sup>3</sup>

<sup>1,2,3</sup>M.Tech, Department of Computer Science & Engineering, Jhulelal Institute of Technology, Nagpur, India

Corresponding Author: pushprajdeshkar68@gmail.com

Available online at: [www.ijcseonline.org](http://www.ijcseonline.org)

**Abstract**— Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

**Index Terms**—Access control, attribute-based encryption (ABE), disruption-tolerant network (DTN), multiauthority, secure data retrieval.

**Keywords**—Internet of Things, machine learning, cloud data, forecasting, load.

### I. INTRODUCTION

Mobile nodes in military environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption-tolerant network (DTN) technologies are becoming successful solutions that allow wireless devices carried by soldiers to communicate with each other and access the confidential information or command reliably by exploiting external storage nodes. Some of the most challenging issues in this scenario are the enforcement of authorization policies and the policies update for secure data retrieval. Ciphertext-policy attribute-based encryption (CP-ABE) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities., we propose a secure data retrieval scheme using CPABE for decentralized DTNs where multiple key authorities manage their attributes independently. We demonstrate how to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption-tolerant military network.

### II. PROBLEM DEFINATION

Military applications require increased protection of confidential data including access control method, 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.

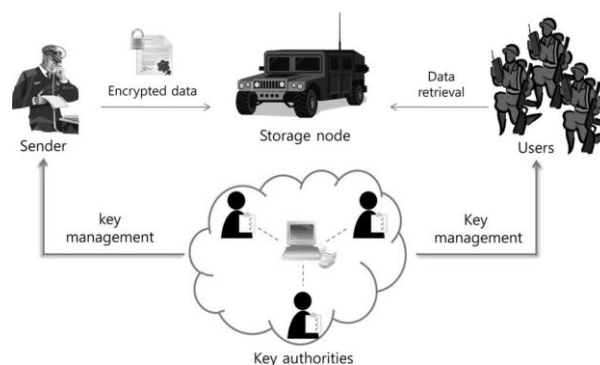


Fig 1. System Flow

### PROPOSED METHOD

1) Key Authorities: They are key generation centers that generate public/secret parameters for CP-ABE. The key authorities consist of a central authority and multiple local authorities. We assume that there are secure and reliable communication channels between a central authority and each local authority during the initial key setup and generation phase. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users’ attributes. The key authorities are assumed to be honest-but-curious. That is, they will honestly execute the assigned tasks in the system; however they would like to learn information of encrypted contents as much as possible.

2) Storage node: This is an entity that stores data from senders and provide corresponding access to users. It may be mobile or static. Similar to the previous schemes, we also assume the storage node to be semitrusted, that is honest-but-curious.

3) Sender: This is an entity who owns confidential messages or data (e.g., a commander) and wishes to store them into the external data storage node for ease of sharing or for reliable delivery to users in the extreme networking environments. A sender is responsible for defining (attribute-based) access policy and enforcing it on its own data by encrypting the data under the policy before storing it to the storage node.

4) User: This is a mobile node who wants to access the data stored at the storage node (e.g., a soldier). If a user possesses a set of attributes satisfying the access policy of the encrypted data defined by the sender, and is not revoked in any of the attributes, then he will be able to decrypt the **IDEA ALGORITHM** and obtain the data. Since the key authorities are semi-trusted, they should be deterred from accessing plaintext of the data in the storage node; they should be still able to issue secret keys to users.

In order to realize this somewhat contradictory requirement, the 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.

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.

### III. METHODOLOGY

We propose an attribute-based secure data retrieval scheme using CP-ABE for decentralized DTNs. The proposed scheme features the following achievements. First, immediate attribute revocation enhances backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptors can define a fine-grained access policy using any monotone access structure under attributes issued from any chosen set of authorities. Third, the key escrow problem is resolved by an escrow-free key issuing protocol that exploits the characteristic of the decentralized DTN architecture. The key issuing protocol generates and issues user secret keys by performing a secure two-party computation (2PC) protocol among the key authorities with their own master secrets. The 2PC protocol deters the key authorities from obtaining any master secret information of each other such that none of them could generate the whole set of user keys alone. Thus, users are not required to fully trust the authorities in order to protect their data to be shared. The data confidentiality and privacy

can be cryptographically enforced against any curious key authorities or data storage nodes in the proposed scheme.

#### IDEA ALGORITHM

IDEA 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" round final Transformation. There are 216 possible 16-bit blocks: 0000000000000000, 1111111111111111, .. Each operation with the set of possible 16-bit blocks is an algebraic group. Bitwise XOR is bitwise addition modulo 2, and addition modulo 216 is the usual group operation. Some spin must be put on the elements – the 16-bit blocks – to make sense of multiplication modulo 216 + 1, however. 0 (i.e., 0000000000000000) is not an element of the multiplicative group.

- Confidentiality: In order to protect sensed data and communication exchange between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information Integrity and Authentication: Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence authentication mechanisms should be "collective" and aim at securing the entire network.
- In particular, the following requirements must be supported by the key management scheme, in order to facilitate data aggregation and dissemination process:

- 1. Data aggregation is possible only if intermediate nodes have access to encrypted data so that they can extract measurement values and apply to them aggregation functions. Therefore, nodes that send data packets toward the base station must encrypt them with keys available to the aggregator nodes.
- 2. Data dissemination implies broadcasting of a message from the aggregator to its group members. If an aggregator shares a different key (or set of keys) with each of the sensor within its group, then it will have to make multiple transmissions, encrypted each time with a different key, in order to broadcast a message to all of the nodes. But transmissions must be kept as low as possible because of their high energy consumption rate.
- Confidentiality : In order to protect sensed data and communication exchanges between sensor nodes it is important to guarantee the secrecy of messages. In the sensor network case this is usually achieved by the use of symmetric cryptography as asymmetric or public key cryptography in general is considered too expensive. However, while encryption protects against outside attacks, it does not protect against inside attacks/node compromises, as an attacker can use recovered cryptographic key material to successfully eavesdrop, impersonate or participate in the secret communications of the network. Furthermore, while confidentiality guarantees the security of communications inside the network it does not prevent the misuse of information reaching the base station. Hence, confidentiality must also be coupled with the right control policies so that only authorized users can have access to confidential information
- Integrity and Authentication : Integrity and authentication is necessary to enable sensor nodes to detect modified, injected, or replayed packets. While it is clear that safety-critical applications require authentication, it is still wise to use it even for the rest of applications since otherwise the

owner of the sensor network may get the wrong picture of the sensed world thus making inappropriate decisions. However, authentication alone does not solve the problem of node takeovers as compromised nodes can still authenticate themselves to the network. Hence authentication mechanisms should be "collective" and aim at securing the entire network.

- First we focused on the establishment of trust relationship among wireless sensor nodes, and presented a key management protocol for sensor networks. The protocol includes support for establishing four types of keys per sensor node: individual keys shared with the base station, pairwise keys shared with individual neighboring nodes, cluster keys shared with a set of neighbors, and a group key shared with all the nodes in the network. We showed how the keys can be distributed so that the protocol can support in-network processing and efficient dissemination, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node. Applying the protocol makes it really hard for an adversary to disrupt the normal operation of the network.

#### IV. CONCLUSION

The corresponding attribute group keys are updated and delivered to the valid attribute group members securely (including the user). In addition, all of the components encrypted with a secret key in the ciphertext are reencrypted by the storage node with a random, and the cipher text components corresponding to the attributes are also reencrypted with the updated attribute group keys. Even if the user has stored the previous cipher text exchanged before he obtains the attribute keys and the holding attributes satisfy the access policy, he cannot decrypt the previous ciphertext.

#### 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 scheme for disruption tolerant networks," in *Proc. IEEE MILCOM, 2006*, pp.
- [3] M. M. B. Tariq, M. Ammar, and E. Zequra, "Message ferry route design for sparse ad hoc networks with mobile nodes," in *Proc. ACM*

- [4] 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.
- [5] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs," in *Proc. IEEE MILCOM*,
- [6] 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.
- [7] Wang, L.M.; Shi, Y. Patrol detection for replica attacks on wireless sensor networks. *Sensors* **2011**, *11*, 2496–2504.
- [8] Zhu, S.; Setia, S.; Jajodia, S.; Ning, P. Interleaved hop-by-hop authentication against false data injection attacks in sensor networks. *ACM Trans. Sensor Netw.* **2007**.