



## Wireless Network Communication Using For Slotted-Aloha Protocol

<sup>1</sup>D. Suba, <sup>2</sup>A. Senthil Kumar

<sup>1</sup>Research Scholar, <sup>2</sup>Asst. Professor

<sup>1,2</sup>Department of Computer Science, Tamil University, Thanjavur, Tamilnadu, India

**Abstract:** The goals of this paper are to derive the optimal transmission probability maximizing a system throughput for both protocols and to develop a simple random access protocol with MPR, which achieves a system throughput close to the maximum value. To this end, we first obtain the optimal transmission probability of a node in the slotted-Aloha protocol. The result provides a useful guideline to help us develop a simple distributed algorithm for estimating the number of active nodes. We then obtain the optimal transmission probability in the persistent CSMA protocol. To deal with the complicated medium access interactions induced by relaying and leverage the benefits of such cooperation, an efficient Cooperative Medium Access Control (CMAC) protocol is needed. In this paper, we propose a novel cross-layer Distributed Energy-adaptive Location-based CMAC protocol, namely DEL-CMAC, for Mobile Ad-hoc Networks (MANETs). A trivial implementation is to let data owners retrieve the data and re-encrypt it under the new access policy, and then send it back to the cloud.

**Keywords:** Node, Security, cloud

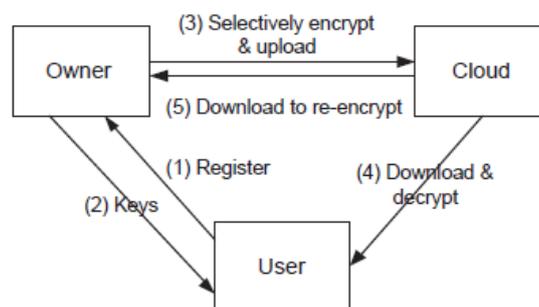
### I. INTRODUCTION

The cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. A better approach should delegate the enforcement of fine-grained access control to the cloud, so to minimize the overhead at the data owners, while assuring data confidentiality from the cloud. We propose an approach, based on two layers of encryption, that addresses such requirement. Under our approach, the data owner performs a coarse-grained encryption, whereas the cloud performs a fine-grained encryption on top of the owner encrypted data. This method, however, incurs a high communication overhead and heavy computation burden on data owners. In this paper, we propose a novel scheme that enabling efficient access control with dynamic policy updating for big data in the cloud.

Typically, when there is no end-to-end connection between a source and a destination pair, the messages from the source node may need to wait in the intermediate nodes for a substantial amount of time until the connection would be eventually established. In cloud computing, users can outsource their computation and storage to servers using Internet.

This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications, infrastructures and platforms to help developers write applications. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced.

Users then are given only the keys for the data items they are allowed to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items.



- 1) Correctness: Users who possess sufficient attributes should still be able to decrypt the data encrypted under new access policy by running the original decryption algorithm.
- 2) Completeness: The policy updating method should be able to update any type of access policy.

3) Security: The policy updating should not break the security of the access control system or introduce any new security problems.

## II. TRANSMISSION PROBABILITY

We assume that the number  $N$  of active nodes is known a priori. In the slotted-Aloha protocol, the channel time is divided into time slots of an equal length. We assume that the length of a packet is constant. A time slot is long enough to accommodate a packet transmission and the corresponding acknowledgement packet.

Since some users may change their associated attributes at some point for example, moving their region, or some private keys might be compromised, key revocation for each attribute is necessary in order to make systems secure. However, this issue is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users henceforth, we refer to such a collection of users as an attribute group. This implies that revocation of any attribute or any single user in an attribute group would affect the other users in the group.

## III. SLOTTED-ALOHA PROTOCOL

We first investigate the optimal transmission probability in the slotted-Aloha protocol with MPR given that the number of active nodes is known to all the nodes. Based on the result, we next present an algorithm for estimating the number of active nodes at runtime in a distributed manner. Combining the algorithm with the result of the optimal transmission probability in the slotted-Aloha leads to an optimal slotted-Aloha protocol, which dynamically and optimally tunes the transmission probability of node depending on the estimated number of active nodes.

### 3.1. Assumptions

The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing user's content, but cannot modify it. This is a valid assumption that has been made. Honest-but-curious model of adversaries do not tamper with data so that they can keep the system functioning normally and remain undetected. Users can have either read or write or both accesses to a file stored in the cloud. All communications between users are secured by secure shell protocol, SSH.

A challenging issue in the TLE approach is how to decompose the ACPs so that fine-grained ABAC enforcement can be delegated to the cloud while at the same time the privacy of the identity attributes of the users and confidentiality of the data are assured. In

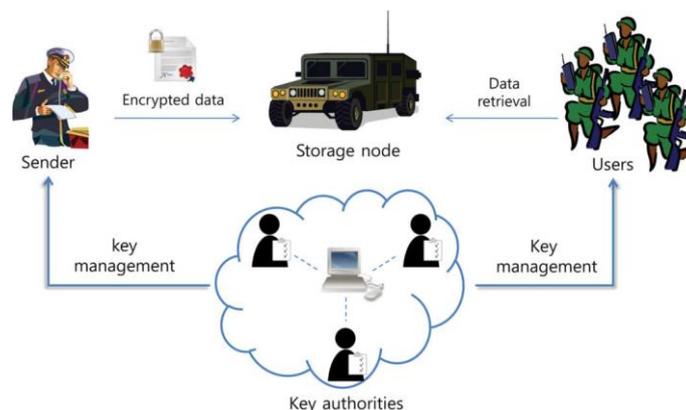
order to delegate as much access control enforcement as possible to the cloud, one needs to decompose the ACPs such that the data owner manages minimum number of attribute conditions in those ACPs that assures the confidentiality of data from the cloud. Each ACP should be decomposed to two sub ACPs such that the conjunction of the two sub ACPs result in the original ACP.

The trade off between the gains promised by cooperation and extra overhead is taken into consideration in the proposed protocol. In addition, in the previous works, very little attention has been paid to the impact brought by varying transmitting power in CC on the interference ranges, since constant transmitting power is generally used. The interference ranges alteration in both space and time will significantly affect the overall network performance.

The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attribute keys to users independently with their own master secrets, it is very hard to define fine-grained access policies over attributes issued from different authorities. Suppose that attributes "role 1" and "region 1" are managed by the authority A, and "role 2" and "region 2" are managed by the authority B. Then, it is impossible to generate an access policy (( "role 1" OR "role 2" ) AND ( "region 1" or "region 2" )) in the previous schemes because the OR logic between attributes issued from different authorities cannot be implemented.

This is due to the fact that the different authorities generate their own attribute keys using their own independent and individual master secret keys. Therefore, general access policies, such as " -out-of- " logic, cannot be expressed in the previous schemes, which is a very practical and commonly required access policy logic.

**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.



Later when a valid user, say Bob wants to modify any of these reports he also attaches a set of claims which the cloud verifies. For example, Bob is a research chair and might send a claim “Research chair” or “Department head” which is then verified by the cloud. It then sends the encrypted data to the Bob. Since Bob is a valid user and has matching attributes, he can decrypt and get back the information.

If Bob wants to read the contents without modifying them, then there is no need to attach a claim. He will be able to decrypt only if he is a Professor in University X or a Research chair in one of the universities X; Y ;Z or a student belonging to Department of Law in university X.

#### IV. SYSTEM AND SECURITY

Consider a cloud storage system with multiple authorities. The system model consists of the following Entities: authorities (AA), cloud server (server), data owners (owners) and data consumers (users).

**Authority.** Every authority is independent with each other and is responsible for managing attributes of users in its domain. It also generates a secret key pair for each attribute in its domain, and generates a secret key for each user according to his attributes.

**Server.** The cloud server stores the data for data owners and provides data access service to users. The server is also responsible for updating ciphertexts from old access policies to new access policies.

**Owner.** The data owners define access policies and encrypt data under these policies before hosting them in the cloud. They also ask the server to update access policies of the encrypted data stored in the cloud. After that, they will check whether the server has updated the policies correctly.

**User.** Each user is assigned with a global user identity and can freely get the ciphertexts from the server. The user can decrypt the ciphertext, only when its attributes satisfy the access policy defined in the ciphertext.

To come up with a reasonable system model, we assume that data connections among terminals are randomly generated and the routes are established by running Ad hoc On-demand Distance Vector, which is a widely used conventional routing protocol for MANETs. There are two types of relay terminals in our network, i.e., routing relay terminals and cooperative relay terminals. In the system model, AODV builds the route in a proactive manner by selecting the routing relay terminals firstly. When a route is established, DEL-CMAC initiates the cooperation in a hop-by-hop manner by selecting the cooperative relay terminals. In this paper, the source and destination terminals are referred to the terminals at MAC layer, and the relay terminals indicate the cooperative relay terminals.

##### 4.1. Detail and Supplement

Elaborate the detail and the supplement of the proposed DEL-CMAC. Specifically, we address the optimal power allocation scheme, the utility-based best relay selection strategy, and the NAV network allocation vector setting in the following subsections.

#### V. CONCLUSIONS

The applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. CP-ABE is a scalable cryptographic solution to the access control and secure data retrieval issues. Key distribution is done in a decentralized way. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user. We have developed an efficient method to outsource the policy updating to the cloud server, which can satisfy all the requirements.

#### 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.1–6.
- [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 MobiHoc*, 2006, pp. 37–48.
- [4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” *Proc. 14th Int’l Conf. Financial Cryptography and Data Security*, pp. 136-149, 2010.
- [5] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” *Proc. First Int’l Conf. Cloud Computing (CloudCom)*, pp. 157-166, 2009.
- [6] C. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD dissertation, <http://www.crypto.stanford.edu/craig>, 2009.
- [7] K. Yang, X. Jia, and K. Ren, “Attribute-based fine-grained access control with efficient revocation in cloud storage systems,” in *AsiaCCS’13.ACM*, 2013, pp. 523–528.
- [8] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, “DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems,” *IEEE Trans. Info. Forensics Security*, vol. 8, no. 11, pp. 1790–1801, 2013.
- [9] H. Shan, P. Wang, W. Zhuang, and Z. Wang, “Cross-layer cooperative triple busy tone multiple access for wireless networks,” *Proc. IEEE Globecom*, pp.1-5, Dec. 2008.
- [10] X. Wang, J. Li, and M. Guizani, “NCAC-MAC: Network Coding Aware Cooperative Medium Access Control for Wireless Networks,” *Proc. IEEE WCNC*, pp. 1646-1651, Apr. 2012.