www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Secure enabled region based data sharing in manet

Guhan.E, Indhu.S Vanitha.M1mrs.Kavitha.M (AP/Sr.GR)
Department of Information Technology
Velalar College of Engineering and Technology, Erode
Email: guhanraja1997@gmail.com

ABSTRACT: Mobile nodes in social environments such as a battlefield or a hostile region are likely to suffer from intermittent network connectivity and frequent partitions. Disruption tolerant network 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. Cipher text policy Anonymous Location Enabled Routing Encryption (CP-ALERT) is a promising cryptographic solution to the access control issues. However, the problem of applying CP-ALERT in decentralized OSN introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. The proposition of a secure data retrieval scheme using CP-ALERT for decentralized OSN where multiple key authorities manage their attributes independently is stated. The demonstration to apply the proposed mechanism to securely and efficiently manage the confidential data distributed in the disruption tolerant military network.

I. INTRODUCTION:

The 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 technologies are becoming successful solutions that allow nodes to communicate with each other in these extreme networking environments. 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. Introduced storage nodes in OSN where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently.

The revocation of any attribute or any single user in an attribute group would affect the other users in the group. Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys. The information that the different authorities generate their own attribute keys using their own independent and individual master secret keys.

With the proliferation of mobile devices, mobile social networks (MSNs) are becoming an inseparable part of our lives. In this application, a user only needs to input some (query) attributes in her profile, and the system would automatically find the person around with similar profiles.

II. LITERATURE SURVEY:

A. *NODE DENSITY BASED ADAPTIVE ROUTING SCHEME*

Traditional ad hoc routing protocols do not work in intermittently connected networks since end-to-end paths may not exist in such networks. A store-and-forward approach has been proposed for delivering messages in disruption tolerant networks. This work revealed that in a single domain environment, even with the custody transfer feature, the delivery ratio drops when the nodes are sparsely connected. They

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

propose a node-density based adaptive routing (NDBAR) scheme that provides better performance than previous approaches.

B. CIPHER TEXT POLICYATTRIBUTE BASED ENCRYPTION

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. In this technique encrypted data can be kept confidential even if the storage server is entrusted moreover this methods are secure against collusion attacks. In this system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message in this system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher text if that user's attributes pass through the cipher texts access structure.

C. DISRUPTION TOLERANT NETWORKING

Disruption Tolerant Networking is a networking architecture that is designed to provide communications in the most unstable and stressed environments. They introduced storage nodes in OSN where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. For example, in a disruption-tolerant military network, a commander may store confidential information at a storage node, which should be accessed by members of "Battalion 1" who are participating in "Region 2."

D. DECENTRALIZING ATTRIBUTE-BASED ENCRYPTION

In this system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A user can encrypt data in terms of any Boolean formula over attributes issued from any chosen set of authorities. Each component in the system will come from a potentially different authority, where it assumed no coordination between such authorities. It creates new techniques to tie key components together and prevent collusion attacks between users with different global identifiers.

E. FUZZY IDENTITY BASED ENCRYPTION

A new type of Identity-Based Encryption (IBE) scheme that they call Fuzzy Identity-Based Encryption is introduced. In Fuzzy IBE an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a cipher text encrypted with an identity, ω0, if and only if the identities ω and ω0 are close to each other as measured by the "set overlap" distance metric. This IBE schemes are both error-tolerant and secure against collusion attacks.

F. SECURE FRIEND DISCOVERY IN MOBILE NETWORKS

Mobile social networks, which bring social networking to mobile phones, represent a natural next step and have already generated a lot of excitement. For example, cell phone manufacturers and cellular service providers have developed their own social networks (*e.g.*, Nokia, Virgin Mobile) and provided software support for mobile social networks (*e.g.*, Motorola). A key component of this solution is the first secure dot product protocol that is both privacy-preserving and verifiable. It has applications beyond mobile social networks because dot product is a fundamental primitive in secure multiparty computation and privacy-preserving data mining.

G. KEYWORD SEARCH AND OBLIVIOUS PSEUDO RANDOM FUNCTIONS

These protocols enable keyword queries while providing privacy for both parties: namely, Hiding the queries from the database (client privacy) and preventing the clients from learning anything but the results of the queries (server privacy). One of their main contributions is a general construction of (relaxed) OPRF from OT. This construction is based on techniques from, yet improves on these works as (1) it preserves privacy against (up to t) adaptive queries, (2) it is obliviously evaluated in constant number of rounds, and (3) it handles exponential domain size.

H. PERFECTLY-SECURE MPC WITH LINEAR COMMUNICATION COMPLEXITY

Secure multi-party computation (MPC) enables a set of n players to securely evaluate an agreed function even when t of the players is corrupted by a central adversary. All the protocols used here are "player elimination"- a technique that enables converting non-robust protocols into robust protocols, essentially without any efficiency loss.

III. PROPOSED SYSTEM

An attribute-based secure data retrieval scheme using CP-ALERT for decentralized OSN. The proposed scheme features the following achievements. First, immediate attribute revocation enhances

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com

backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryption 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 OSN 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.

IV. MODULE DESCRIPTION:

The Efficient **CP-ALERT - Cipher Text Policy Based Anonymous Location Enabled Routing** provides to mainly focus as following Modules,

1. Non-Predictional Ranging

CP-ALERT Ranging, nodes move in straight lines until either enough ranges are collected. The first step, Synchronization, allows participating nodes to calculate the difference in their clocks. The second step, Transmission, provides the ranging signal. The final step, Data Exchange, involves an exchange of data that terminates with both nodes aware of the range between themselves we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. CP-ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

2. SECURE SYNCRONIZATION

In the Synchronization step of ranging, nodes A and B exchange two packets. Node A sends a request packet containing a nonce encrypted with the pair wise key AB and the hash of a second nonce. The packet is authenticated using a message authentication code generated using pair wise key AB. Node B responds with a packet containing the decrypted nonce that is also authenticated. Both nodes store the transmission and reception time of the two packets. A node use NAK to acknowledge the loss of packets.

3. ALERT TRANSMISSION

The Transmission step, node A ranges by sending a preamble followed by each individual bit of nonce Ns at predetermined intervals. Node B records the arrival time of the preamble and assembles the bits to reconstruct the nonce. Node A encrypts and sends a packet to node B through RF containing timing information and distance, traveled since the last ranging operation. Nonce Ns is also sent in order to properly associate sets of timing data. Node B stores this data until all ranges are complete and computes its range to A using the ranging signal velocity s.

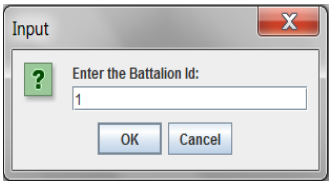
4. PACKET VERIFICATION

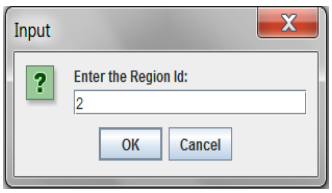
Verification uses preliminary checks, metric multidimensional scaling (MDS) and knowledge of node movement to detect distortions caused by a channel load by attacker. CP-ALERT is used to analyze ranges and traveled distances to determine if a channel load by attacker has affected the results. Successful verification confirms that the two nodes are neighbors.

5. KEY AUTHORITIES

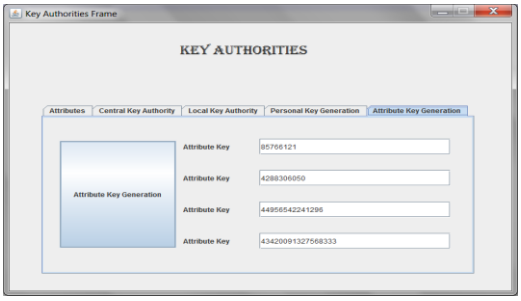
They are key generation centers that generate public/secret parameters. The key authorities consist of a central authority and multiple local authorities. Each local authority manages different attributes and issues corresponding attribute keys to users. They grant differential access rights to individual users based on the users attributes.

SCREENSHOTS FOR OUTPUT:





Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com



V. CONCULSION:

Ciphertext Policy Attributebased Encryption (CP-ABE), is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The data owner defines the access policies and encrypts data according to the policies. Each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the access policies. Proposing a revocable multi authority CP-ABE scheme, where an efficient and secure revocation method is proposed to solve the attribute revocation problem in the system.

1. Modify the framework of the scheme and make it more practical to cloud storage systems, in which data owners are not involved in the key generation.

2. Greatly improve the efficiency of the attributer vocation method.

VI. REFERENCES:

[1] M.Chuahand P. Yang, "Performance evaluation of content based information retrieval schemes for OSN," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[2] M.ChuahandP.Yang, "Node density-based adaptive routing scheme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp. 1– 6.

[3] P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,''National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[4] Ing-Ray Chen,Dynamic Hierarchical TrustManagement of Mobile Groups and Its Application to Misbehaving Node Detection" Dept. of Computer. Sci., Virginia Tech, Blacksburg.

[5] M.Chase,"Multiauthority attribute based encryption," in Proc. TCC, 2007, LNCS 4329, pp.515–534.

Copyrights © International Journal of Intellectual Advancements and Research in Engineering Computations, www.ijiarec.com