Secure Range Free Authentication for Wireless Sensor Network

Mrs. K. Vijaya -AP(Sr. Gr) /CSE
Elam Atchaya. A, Krishnapriya. V, Gowtham. S
Velalar College of Engineering and Technology, Thindal, Erode.

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 (OSN) 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.**

1.INTRODUCTION

DISRUPTION TOLERANT NETWORK

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 (OSN) 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.

ATTRIBUTE BASED ENCRYPTION

The concept of attribute-based encryption is a promising approach that fulfills the requirements for secure data retrieval in OSN. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, ciphertext-policy ABE provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy. However, the problem of applying the ABE to OSN introduces several security and privacy challenges. 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 (or update) for each attribute is necessary in order to make systems secure. However, the subject is even more difficult, especially in ABE systems, since each attribute is conceivably shared by multiple users (henceforth, referring to such a collection of users as an attribute group).keys to users' associated set of attributes. Thus, the key authority can decrypt every ciphertext addressed to specific users by generating their attribute keys.

If the key authority is compromised by adversaries when deployed in the hostile environments, this could be a potential threat to the data confidentiality or privacy especially when the data is highly sensitive. The key escrow is an inherent problem even in the multiple-authority systems as long as each key authority has the whole privilege to generate their own attribute keys with their own master secrets. Since such a key generation mechanism based on the single master secret is the basic method for most of the asymmetric encryption systems such as the attribute-based or identity-based encryption protocols, removing escrow in single or multiple-authority CP-ABE is a pivotal open problem. The last challenge is the coordination of attributes issued from different authorities.

When multiple authorities manage and issues 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. For example, 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. The information 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.

2.EXISTING SYSTEM

The concept of attribute-based encryption is a promising approach that fulfills the requirements for secure data retrieval in OSN. ABE features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and cipher texts. Especially, Ciphertext policy ABE provides a scalable way of encrypting data such that the encryptor defines the attribute set that the decryptor needs to possess in order to decrypt the ciphertext. Thus, different users are allowed to decrypt different pieces of data per the security policy.

DISADVANTAGES OF EXISTING SYSTEM

The problem of applying the ABE to OSN introduces several security and privacy challenges. 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 (or update) 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)

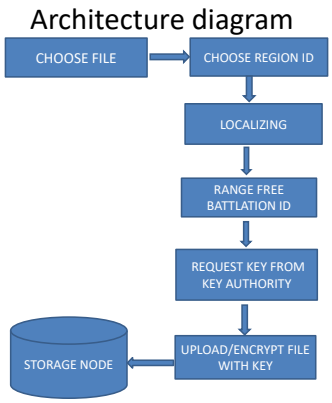
Another challenge is the key escrow problem. In CP-ABE, the key authority generates private keys of users by applying the authority's master secret keys to users' associated set of attributes.

4. The last challenge is the coordination of attributes issued from different authorities. When multiple authorities manage and issue attributes 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.

3.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 backward/forward secrecy of confidential data by reducing the windows of vulnerability. Second, encryptor 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

ADVANTAGES OF PROPOSED SYSTEM



Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node. In addition, unauthorized access from the storage node or key authorities should be also prevented.

Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

4.PROJECT ANALYIS AND RESULTS

There are partitions in military environments such as a battlefield or a hostile region. They are likely to suffer from intermittent network connectivity which is having frequent partitions. Disruption-tolerant network OSN technologies are is a true and easy solution. OSN is a Disruption-tolerant network. It allows devices which are wireless and carried by peoples in a military to interact with each other. These devices access the confidential information or command reliably by exploiting external storage nodes. In these networking environments OSN is very successful technology. When there is no wired connection between a

source and a destination device, the information from the source node may need to wait in the intermediate nodes for a large amount of time until the connection would be correctly established. One of the challenging approaches is the ABE. That is attribute-based encryption which fulfills the requirements for secure data retrieval in OSN. The concept is Cipher text Policy ALERT (CP-ALERT). It gives an appropriate way of encryption of data. The encryption includes the attribute set that the decryption needs to possess in order to decrypt

the cipher text. Hence, many users can be allowed to decrypt different parts of data according to the security policy.

Computation and communication costs:

A significant fraction of the computation in L3P can be done offline. In addition, as mentioned before, some computation and communication can be done in parallel, thus reducing the overall protocol execution time. In the proposed L1P, the Initiator executes part of the protocol offline which in turn reduces the online computation cost. As the computational complexity of the exponentiation operation dominates the other operations like multiplication and addition, analyze the computation overhead focusing on exponentiation operations.

ASYMMETRIC SOCIAL PROXIMITY MEASURE VALIDATION

An asymmetric social proximity metric between two users is proposed, which is based on each user's as well as his/her friends' perceptions on the common communities between the two users. The ego-network has 556 nodes(A's friends) and 7,856 edges (interconnections among A's friends). The degree of each node in the network gives the number of common friends between A and the node (A's friend). Note that A is not in the network. In order to quantify the proximity between A and any of his friends according to the asymmetric proximity metric proposed in this paper, A divides his friends into the following six friend circles:

Friends from hometown,

Friends in the current university,

Friends from the previous university,

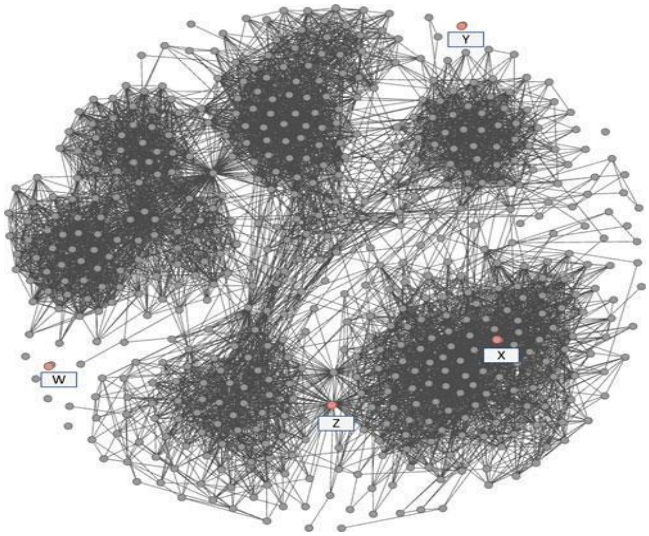
Job 1 friends,

Job 2 friends,

Others.

For example, Z and X share approximately the same number of friends with A, and their normalized numbers of common friends with A. In contrast, the proposed asymmetric proximity of Z is nearly twice as much as that of X since Z shares two communities with A and belongs to two different friend circles while X only shares one community with A and belongs to only one friend circle. The higher social proximity value of Z is justified from the network theory perspective. Particularly, the ratio of between's centrality of Z to that of X which emphasizes the relative importance of node Z over X. Similarly, the normalized number of common attributes fails to well differentiate the importance of friends as well. Most nodes have the same normalized number of common attributes, and hence cannot be differentiated based on this metric. More importantly it also fails to fully establish friendships whenever possible. For example, many of A's friends do not have any common attributes with A and hence their normalized numbers of common attributes are 0. On the other hand, the proposed asymmetric proximity measure gives non-zero values as those friends share attributes with some other friends of A. The experiment confirms our argument in the beginning that whether two people can become friends not only depends on whether they have anything (attributes) in common, but also depends on whether their friends have anything in common. To give another example, A's friends W and Y have same normalized number of common friends and the same number of common attributes. In contrast, the proposed asymmetric proximity measure is able to differentiate these two friends, as they are associated with different communities and belong to different friend circles with different sizes and weights. Moreover, we conduct similar experiments on ego-networks of Z, as shown.Apparently, the results show that Z values the friendship with A more than A does.

Besides, A is in two of the total four different friend circles of Z, whereas Z is in two of the six friend circles of A. This demonstrates the asymmetric characteristics of friendships captured by our proximity measure.



ADVANTAGES OF PROPOSED SYSTEM

Data confidentiality: Unauthorized users who do not have enough credentials satisfying the access policy should be deterred from accessing the plain data in the storage node.

In addition, unauthorized access from the storage node or key authorities should be also prevented.

Collusion-resistance: If multiple users collude, they may be able to decrypt a ciphertext by combining their attributes even if each of the users cannot decrypt the ciphertext alone.

Backward and forward Secrecy: In the context of ABE, backward secrecy means that any user who comes to hold an attribute (that satisfies the access policy) should be prevented from accessing the plaintext of the previous data exchanged before he holds the attribute. On the other hand, forward secrecy means that any user who drops an attribute should be prevented from accessing the plaintext of the subsequent data exchanged after he drops the attribute, unless the other valid attributes that he is holding satisfy the access policy.

5.MODULES DESCRIPTION

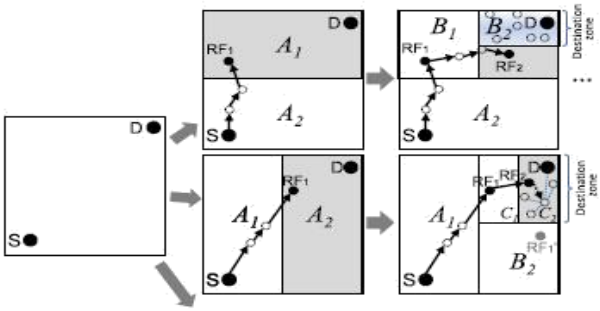
The Efficient CP-ALERT - Cipher Text Policy Based Anonymous Location Enabled Routing provides to mainly focus as following Modules,

NON-PREDICTIONAL

1 RANGING
2 SECURE SYNCRONIZATION
3 ALERT TRANSMISSION
4 PACKET VERIFICATION
5 KEY AUTHORITIES

NON-PREDICTIONAL RANGING

The main key requirement of the ranging phase is that each ranging node must travel along a describable path. For the purposes of this CP-ALERT Ranging, nodes move in straight lines until either enough ranges are collected or it is no longer possible to range. Ranging operations stop before completion of the protocol when nodes are no longer in contact or when a node is forced to turn. 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. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. The partition process is stated as hierarchical zone partition. 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



5.2 SECURE SYNCHRONIZATION

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. For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet. The packet formats of ALERT, which omits the MAC header. Because of the randomized routing nature in ALERT, a universal format for RREQ/RREP/NAK has proposed. Anode use NAK to acknowledge the loss of packets. The data field of RREQ/RREP is left blank in NAK packets. Flooding based anonymity routing usually uses ACKs, while NAKs are often adopted in geographic routing-based approaches to reduce traffic cost. For the same purpose, decisions to use NAKs have been taken. In the packet, PS is the pseudonym of a source; PD is the pseudonym of the destination; LZS and LZD are the positions of the Hth partitioned source zone and destination zone, respectively. The protection of source anonymity and will be introduced as follows:

The zone position of ZD, i.e., the Hth partitioned zone.

The encrypted zone position of the Hth partitioned zone of S using D's public key, which

is the destination for data response.

The current randomly selected TD for routing.

A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF.

CP-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.

Transmission:

Node A encrypts and sends a packet to node B via RF containing timing information and distance dA, 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.

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.

Verification begins with preliminary checks that include a check for ranges that are too long, adjoining ranges whose length differs by more than the combined distances traveled by the participating nodes, and degenerate configurations. Successful preliminary checks are followed by a loop that performs distance analysis using MDS and a test of the fit of the resulting coordinates. The output is analyzed and the best two outcomes are used to make a decision about the presence/absence of a channel load by attacker.

The first step of Verification is a set of preliminary checks that analyze the distances for easily detectable evidence of channel load by attacker involvement. Preliminary checks include:

$r_i > RRNG + \epsilon$. Ranges as large as $2 \times RRNG$ +delay may be produced by a channel load by attacker. Ranges that exceed RRNG by some defined threshold violate the propagation properties of the ranging signal.

$r_{i+1} = R_i \pm dA_i \pm dB_i$. When all points are collinear, the change in length of consecutive ranges is the direct results of adding and/or subtracting node travel distances.

$(r_i - dA_i - dB_i) < r_{i+1} < (r_i + dA_i + dB_i)$. The length of range r_{i+1} can be no greater than the

sum of ri and the distance traveled by each node between ranges. It can be no smaller than their difference.

4) $(r_i = r_{i+1} = r_{i+2})$ & $(\Sigma r_{i=1} dA_i = \Sigma r_{i=1} dB_i)$. If all ranges are equal and traveled distances are equal, then the graph produced is not rigid.

CP-ALERT uses protocol specifications in standard notation as a guideline for creating a formal syntax. The fundamental aspect of any protocol is its send operator, but CP-ALERT makes the matching receive operator equally important; where standard notation assumes to receive succeeding a send, this makes such assumptions explicit.

The algorithm uses a queue structure to maintain the ordering of sends and receives that works as follows. A sender uses a send statement that places the sent message on the
receiver's queue. The send should be viewed as taking a value in the sender's address space and making it available to the receiver. The receiver explicitly extracts this value from the front of the queue with a receive statement; this places the value in the receiver's address space.

The analyst has a rigorous proof mechanism which can be used to determine if a protocol attains its security goals. Borrowing concepts from programming language design, the analyst develops a formal syntax to represent the protocol steps and semantics to reason about the meaning of these steps. The CP-ALERT, an existing formal methods environment developed specifically for security protocol analysis. In the following sections, we introduce CP-ALERT and our use of it in the analysis of LBRP.

CP-ALERT uses protocol specifications in standard notation as a guideline for creating a formal syntax. The fundamental aspect of any protocol is its send operator, but CP-ALERT with LBRP makes the matching receive operator equally important; where standard notation assumes a receive succeeding a send; CP-ALERT makes such assumptions explicit. It uses a queue structure to maintain the ordering of sends and receives that works as follows. A sender uses a send statement that places the sent message on the receiver's queue. The send should be viewed as taking a value in the sender's address space and making it available to the receiver. The receiver explicitly extracts this value from the front of the queue with a receive statement; this places the value in the receiver's address space. The queue structure enforces an ordering of alternating send and receives statements.

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.

COMPARISION CHART:

PAPER NAME	METHODOLOGY ADOPTED	ADVANTAGES	DISADVANTAGES
Node density based adaptive routing scheme	2 hop relay protocol	Multiple copies to relay nodes and when they encounter destination the relay nodes deliver to it.	End to end connection is not guaranteed. It provide temporary storage.
Cipher text policy attribute based encryption	Role-Based Access Control (RBAC)	Encrypted data can be kept confidential even if the storage server is entrusted.	The drawback is increasingly difficult to guarantee the security of data.
Identity based encryption with efficient revocation	Identity Based Encryption (IBE)	It improves key-update efficiency on the side of the trusted party.	This solution does not scale well as the number of users increases, the work on the key updates becomes a bottleneck.
Improving privacy and security in multi-authority	Attribute Based Encryption (ABE) scheme	It removes the trusted central authority and protects the users privacy by preventing the authorities from pooling their information on particular users	The attribute is valid only it works properly.

CONCLUSION:

Cipher text-Policy Attribute-based 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 authority can be the registration office in a university, the human resource department in a company, and so on. 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.

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.

Greatly improve the efficiency of the attributer vocation method

REEFERENCES

[1] M. Chuah and P. Yang, “Performance evaluation of content-based information retrieval schemes for OSN,” in Proc. IEEE MILCOM, 2007, pp. 1–7.
[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] 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 Trust Management of Mobile Groups and Its Application to Misbehaving Node Detection” Dept. of Comput. Sci., Virginia Tech, Blacksburg.
[5] M. Chase, “Multi-authority attribute based encryption,” in Proc. TCC, 2007, LNCS 4329, pp. 515–534.