An Efficient and Secure Data Retrieval in Wireless Sensor Networks

S. Kodimalar,
P.G Scholar Department of Computer Science and Engineering St.Peter's College of Engg & Technology
Chennai, India

M. Grace Prasana,
Assistant Professor Department of Computer Science and Engineering St.Peter's College of Engg & Technology
Chennai, India

***Abstract*- Mobile nodes in the military environment such as battlefield or hostile region are suffered from a frequent partition and irregular network. Disruption-tolerant network (DTN) is becoming a promising and successful solution for the intermittent network connectivity and other network related problem. The soldiers in the military environment are allowed to communicate each other and access the confidential information by using the storage node in DTN. Ciphertext Policy Attribute-Based Encryption (CP-ABE) is an extremely powerful asymmetric encryption mechanism and promising cryptographic solution to access control issues. Localizability-aided localization (LAL) is a fine-grained approach which does adjustment in network. In this paper, we propose a secure and efficient data distribution and retrieval using CP-ABE and localizability-aided localization (LAL) for decentralized DTNs where multiple key authorities manage their attributes individually. This scheme will manage the attribute effectively and provide more security for soldiers to access confidential information.**

Keywords: DTN, CP-ABE, LAL, Access Control

I. INTRODUCTION

A. Overview

Security is the major concern in defense communication. Military scenario uses wireless device for communication, this may leads to some connection problem in unstable environment. Localization is the major concern in wireless devices used in military communication. To overcome such problems Localizability Aided Localization (LAL) is used, and for security purpose Ciphertext Attribute Based Encryption (CP-ABE) is used in Disruption Tolerant Network. LAL protocol will manage the sensor nodes by adjusting the network, and it will reduce the packet loss.

B. Disruption Tolerant Network

In many military network scenario, wireless devices connection carried by the soldiers may be temporarily disconnected by environmental factors, mobility, and jamming. Disruption Tolerant Network (DTN) is becoming successful solutions that allow the mobile node to communicate each other in stressed and unstable environment. DTN is a network designed so that intermittent or temporary communications problems, anomalies and limitations have the least possible adverse impact. Typically, when there is no end-to-end connection between a destination and source, 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. To overcome the packet loss in the end to end connection storage node [2] is introduced in DTN can store the data where authorized mobile node accesses the information quickly and efficiently. Effective design of a DTN includes several aspects they are:

- Graceful degradation ability under adverse conditions or extreme traffic loads.
- Minimal latency ability to function even when routes are ill-defined or unreliable.
- Fault-tolerant methods and technologies usage.
- The ability to prevent or quickly recover from electronic attacks.

C. Ciphertext Attribute Based Encryption

The concept of Attribute-Based Encryption (ABE) [2] is a promising cryptographic approach that fulfills the requirement of for secure data retrieval in DTNs. It is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. ABE mechanism enables an access control over encrypted data using access policies and described attributes among private keys and cipher text. This approach achieves a fine-grained data access control. Especially Ciphertext attribute based encryption (CP-ABE) provides a secure and scalable way of encrypting data where encryptor defines that attribute set that the decryptor possesses inorder to decrypt the cipher text.

D. Access policy

Access tree is used to represent the access control policy, in which inner nodes are either AND or OR. Boolean operators and leaf nodes are attributes. The decryptor needs to posses the combination of attributes which access tree consists to decrypt an encrypted message under the access tree, the decryptor must possess a secret key which is associated with the attribute set which satisfies. Attributes are interpreted as

logic variables, and possessing a secret key associated with an attribute makes the corresponding logical variable true. Access tree can be satisfied by several different set up attributes.

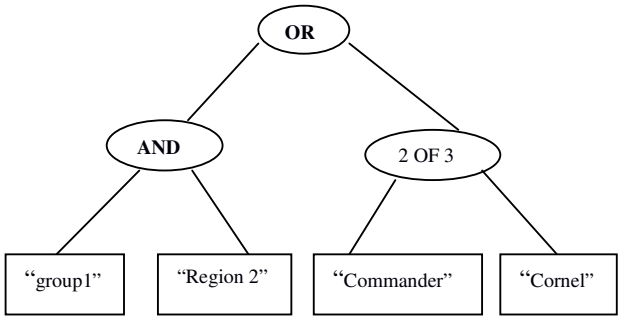

Figure 1: Access Policy

Many military applications require increased security of private information including access control methods that are cryptographically implemented which should be accessed by "group1" who are participating in "Region 2." In this situation it is a sensible supposition that multiple key authorities are likely to manage their own dynamic attributes for users in their regions, than can be frequently changed (e.g., the attribute representing current location of moving soldiers) [6]. In DTN architecture multiple key authorities issue and manage their own attribute keys independently as decentralized [5].

E. Localizability-aided localization (LAL)

Localizability-aided localization (LAL) is a fine-grained approach used for network deployment and adjustment. This approach will manage the military network effectively. LAL triggers a single round adjustment, and then some localization methods can be successfully carried out. The network will be more secure and efficient by using different phases of this approach [14].

F. Network Simulation

ns (Version 2) are an open source of network simulation tool. Ns2 is written in C++ and Otcl languages. The primary use of NS is in network researchers to simulate various types of wired/wireless local and wide area networks; to implement network protocols such as transfer control protocol, traffic behavior such as file transfer protocol, Router queue management mechanism such as drop; routing algorithms like Dijkstra algorithm can be used. To separate the control and data path implementations ns2 is written in otcl and c++. The network simulator supports a class hierarchy in C++ (the compiled hierarchy) and a corresponding hierarchy within the Otcl interpreter. This is the reason ns2 uses two languages are that different tasks have different requirements: For example simulation of protocols requires efficient manipulation of bytes and packet headers making the run-time speed is a very important one here. In network studies, the aim may vary some parameters and to quickly examine a number of scenarios the time to change the model and run it again is more important. In ns2, C++ is used for specified implementation and in general for such cases where every packet of a flow has to that has been processed. If you want to implement a new queuing discipline then we can use C++ as the language of our choice.

II. RELATED WORKS

A. Attribute Revocation

Recently, several attribute revocable ABE schemes have been proposed [3], [5], [10]. Revocation is revoking attribute using expiration time of the attribute. This is called coarse-grained revocation because immediate rekeying on any member is not possible. The first problem is the security degradation in terms of backward and forward secrecy [11]. Soldiers in the military environment may often change their attributes, e.g., location or position when considering these as attributes. Backward secrecy is the user who holds the new attribute might be able to access the previous data encrypted before he obtains the attribute until the data is reencrypted with the newly updated attribute keys. On other hand, a revoked user can still decrypt the previous ciphertext until it is reencrypted with updated attribute key it is known as forward secrecy. Another issue to this approach is scalability. The update of a single attribute affects the whole nonrevoked user who shares the attribute when the key authority announces key update.

B. Key Escrow

ABE schemes are constructed based on the single trusted authority architecture in existing. Single trusted authority has the power to generate the whole private keys of users with its master secret information [8]. Key escrow is considered as a security risk because key authority is given access to decrypt every ciphertext addressed to users in the system by generating secret keys [9]. In the multi authority system, key escrow problem is solved when it is fully distributed. One disadvantage of fully distributed approach is the performance degradation.

C. Decentralized ABE

Decentralized CP-ABE in the multi-authority network environment is distributing the powers of central authority to several local authorities [2]. Combined access policy is achieved over the attributes issued by different authorities by encrypting data multiple times. Efficiency and expressiveness of access policy are the disadvantages of this approach. Using Decentralized ABE will create problem over DTN network. There will not be any central authority, and fully distributed approach lacks efficiency and responsiveness.

D. Limitations of Existing System

- The issue of applying the ABE to DTNs presents a few privacy and security challenges. Since a few user may often change their attribute. Key update is important to make the framework secure.
- Another threat is key escrow issue. In CP-ABE, the key master creates private keys of client by applying the master secret key to clients related set of attributes.
- Coordination of multiple authorities is another issue. Fine grained access policy will not work.

III. ZONE FORMATION

In decentralized disruption tolerant network, every mobile node is combined to form zone with their neighboring node. This is done after finding the sink. Each mobile node will find their zone by their respective range. This is done using zone routing protocol, this protocol will help in forming zones. The zone formation in distribution environment will help the node to deliver the message quickly and effectively. ZRP is a hybrid Wireless networking routing protocol that uses both proactive and reactive routing protocol when sending information over the network. This protocol reduce processing overhead and speed up delivery. This communicates within the zone and between the zones.

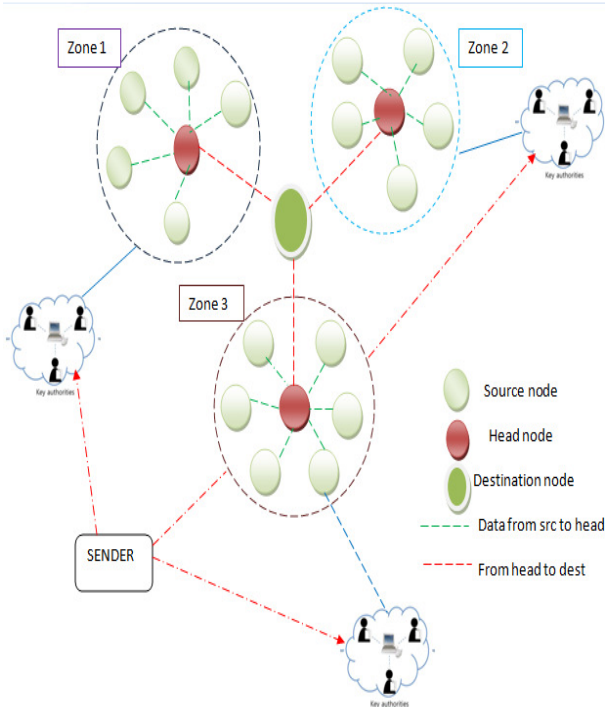

Figure 2: Data Retrieval between Sink and Storage Head

IV. SELECTION OF STORAGE HEAD

After the zone formation each zone will be processes to select their own storage head for each zone. This will be done using broadcasting; it is a process of sending data to all nodes within a zone or limited area. Every node will send messages within their zone, if a node withstand for maximum request from all neighbor nodes within the zone without dropping the data it is selected as storage node. Every zone will select a storage node for communicating with sink node. The storage node can be changed based on the removal of user and addition of new user within the zone

V. CP-ABE POLICY

In ciphertext policy attribute-based encryption, the encryptor can alter the arrangement, which can decrypt the encrypted data or message. This can be done using attributes. In CP-ABE, access policy is sent along with the ciphertext. CP-ABE proposes a fine-grained access rights to gain entrance approach requires not to sent alongside the ciphertext, by which we have the capability to secure the encryptor. This approach encrypts information might be kept classified regardless of the fact that the external storage server is untrusted; besides, our methods are secure against a harmful attacker. We have a tendency to store our file on remote servers. We do this to supply scalable access to our files. In the case of failures, to achieve dependency we want to duplicate our files totally different information organization or different centers. However, we need security for our files. The factor is, there is a tension between security and the alternative properties. We need a lot of trust towards the server to replicate our file and to introduce potential points of compromise. Here in CP-ABE the attributes of the secret key are mathematically incorporated into the key, after encrypting the file; say we put it on the server. Access decision is not explicitly evaluated. Instead, if the policy is satisfied, the user can decrypt the file, otherwise they cannot.

VI. DATA RETRIVAL

The data transfer is done by sender, key authorities, storage node and sink. Sender is an element who stores the confidential information into the outer information storage node in encrypted form for simplicity of sharing. A sender will define the access policy for every user based on their attributes. The storage node will get the encrypted content from the sender and provide access to the users. The storage node is selected by broadcasting. The sink node will communicate only with the storage node to get the secure data. Rather than storage node other mobile nodes cannot directly communicate with the sink. Key authority is a one who will generate keys and distribute those keys according to the users attributes. Based on the individual rights they grant differential access rights.

VII. LOCALIZABILITY AIDED LOCALIZATION (LAL):

Localization is an enabling technique for sensor network application. Physical world positioning demonstrates that, a network is not always localizable; it may leave a certain number of nonlocalizable nodes. We propose a localizability-aided localization (LAL), a fine-grained approach for military network. Here Localization (within border) and non-localization (outer border) nodes of the network are managed to overcome attacks in military network. In LAL, network is deployed randomly and managed effectively by three phases they are: node localizability testing, tree structure analysis, and network adjustment. This approach is suitable for wireless ad hoc and sensor network. Fig 3, shows the work flow of LAL

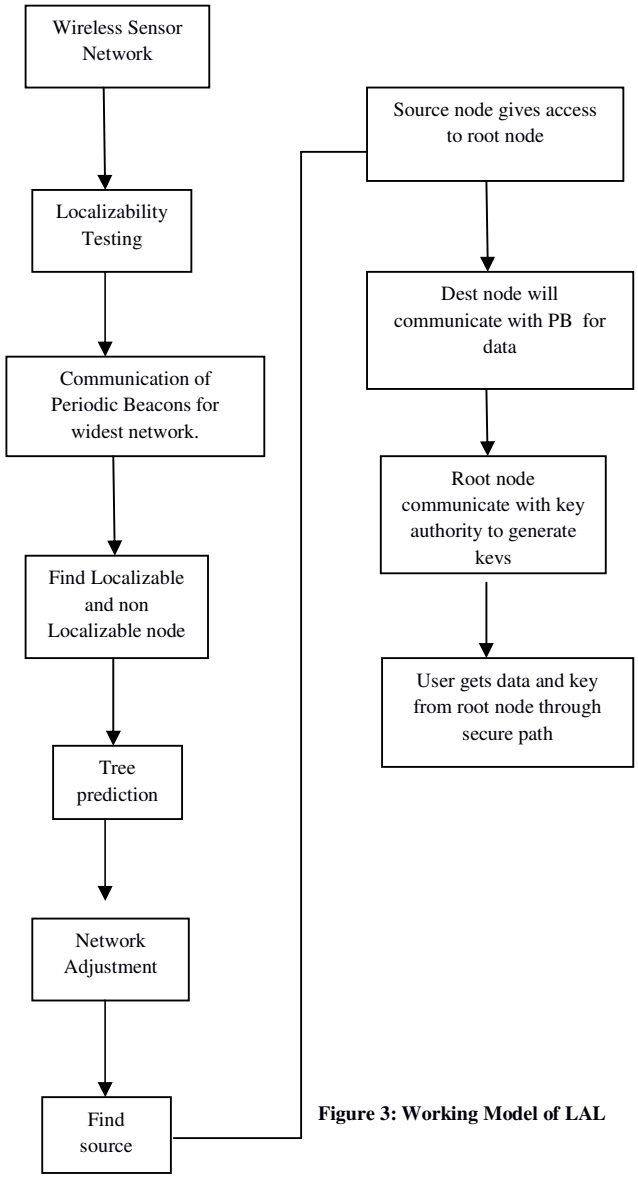

Figure 3: Working Model of LAL

A. *Localizability testing*

When a network is deployed in an application field, due to the environmental factor it may not be ready for localization. Therefore, node localizability testing is first conducted in LAL, which identifies localizable and non-localizable nodes in a network for further adjustment. this testing is also useful in overcoming attacks.

B. *Structure analysis*

In structure analysis, to achieve fine-grained manipulation, the graph distance is decomposed into two connected components. These connected components are organized to form a tree structure that contains a root, which sends instruction to all nodes.

C. *Distinctive adjustment:*

Based on the localizability of nodes LAL treats each node differently. This phase of LAL converts all non-localizable nodes in one round. LAL make adjustments according to the results of node localizability.

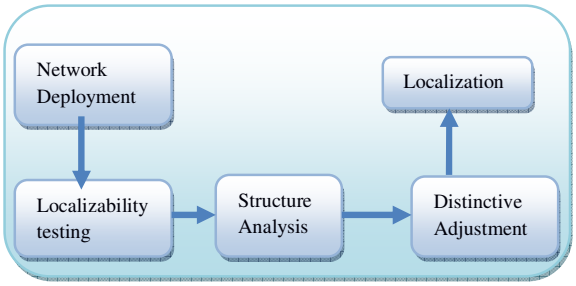

FIGURE 4: Phases of LAL

VIII. IMPLEMENTATION

Since wireless technology and the protocols used are very complex and costly they can't be tested in a reality. In order to overwhelm this issue we are using network simulation-2 software (ns2). With the help of this simulation software we can find out the problems in draft, we can find the volume, few new ideas and different approaches. For WSN and adhoc network design we need three components they are Network, source and target. In decentralized CP-ABE ns2 simulator generates required realistic network performance.

In Decentralized CP-ABE, initially all the sensor nodes are mobility in nature, frequency has been using the ns2-simulating software set to construct the zone formation. Based on the frequency all the sensor nodes try to form zones, based on ZRP protocol all the sensor nodes joins particular group.. After formation of zone, storage node is selected. The node withstands the maximum request is selected as storage node.. After every node will communicate with storage head and

send message to the sink node. Storage node will store the message, if user needs the message he should satisfies the access policy created for his attributes, to retrieve the data. The storage node is the trusted external medium to transfer activity is carried out from source to destination. Here LAL Protocol is proposed to cover the network within the border and outer border. The three phases in LAL is implemented in ns2 to show the efficiency of the protocol. The network of military environment will be adjusted frequently using LAL Protocol. Fig 5, shows the Network adjustment. For routing in LAL we use GPSR (Greedy Perimeter Stateless Routing), this method will find the best neighboring node and it prevents attack. APU (Automatic Position Update) is used by GPSR to update the each sensor node location and tell about the update to the root node. LAL is a fine grained approach uses regressive algorithm, which sense the nodes based on the space and how quickly the information is shared Fig 6 shows the communication between the beacons.

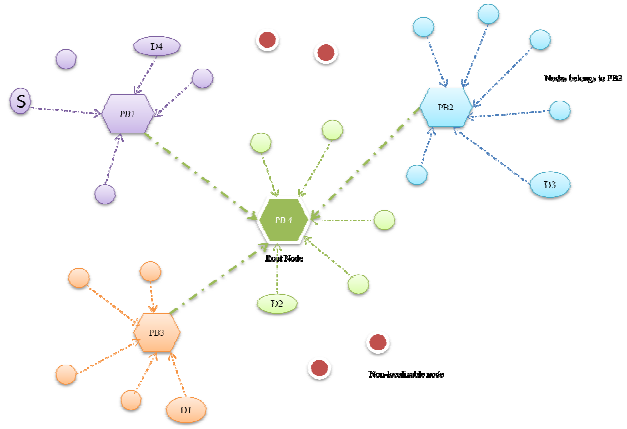

Figure 5: Communication between Beacons and Root Node

IX. EXPERIMENTAL RESULTS AND DISCUSSION

The performance is much better when compared to others which use LAL protocol.

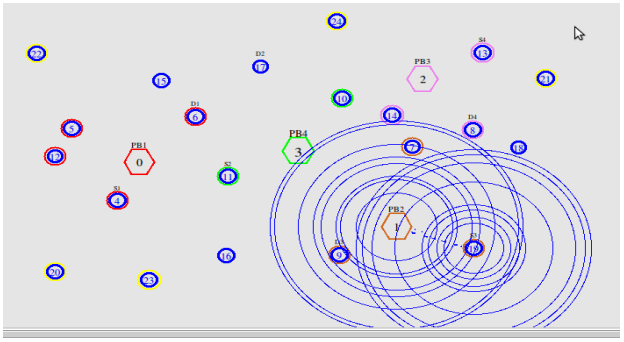

Figure 5: Network Adjustment

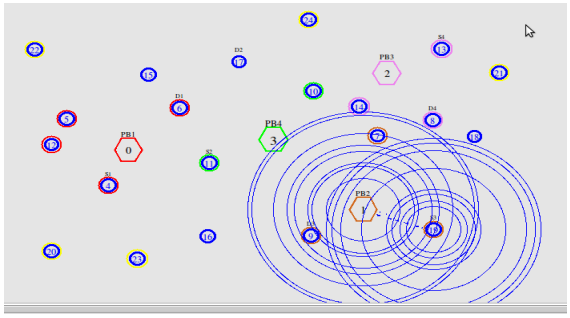

Figure 6: Communication between Beacons

Comparing to the other approaches in military network, LAL perform effectively localizability and non-localizability. We can also support large number of nodes outside the border and within the border. LAL reduces the packet loss and delay. This makes the military network more efficient and faster when compared to other protocols. Fig 8, Shows the comparing graph for the packet loss using LAL protocol and ZRP Protocol. Fig 9 shows the delay ratio of LAL and ZRP. From these graph, we conclude that using LAL protocol we can efficiently communicate in military environment. For routing in LAL, we use GPSR (Greedy Perimeter Stateless Routing) for finding best neighbor this will make LAL more efficient.

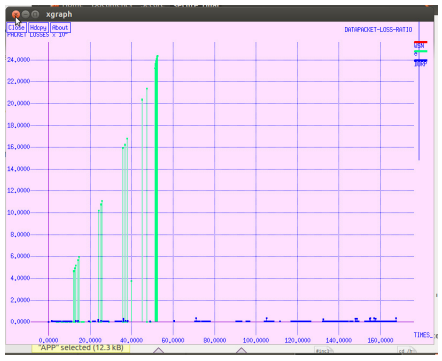

Figure 7: Packet loss Ratio of LAL

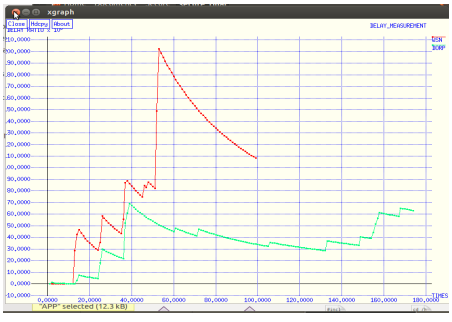

Figure 8: Delay Ratio of LAL

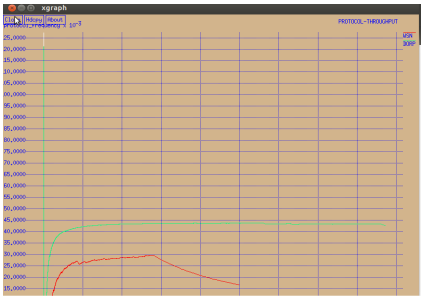

Figure 9: Protocol Efficiency

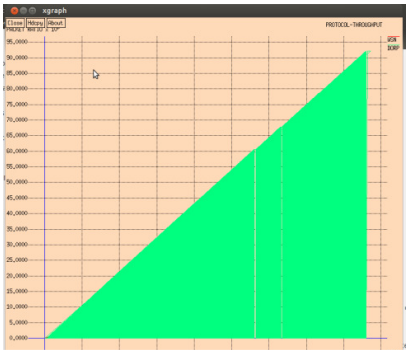

Figure 10: LAL Protocol Throughput Ratio

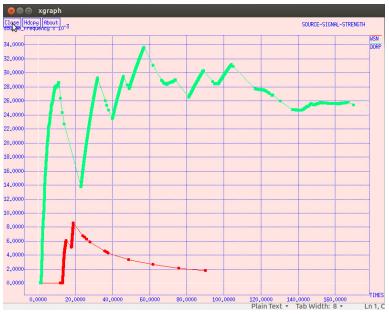

Figure 11: Signal Strength Ratio of LAL

CONC LUSION

In this paper, CP-ABE is proposed for decentralized military network for efficient and secure data retrieval. Other than CP-ABE, LAL is introduced in military network to make the environment more secure. Hence LAL protocol will deploy the network randomly, make adjustments according to node localizability results, other than indistinctively consider the network as a whole. This approach reduces the load on the environment and results in fast response. Therefore these schemes reduce the stress in military environment and provide more security for data distribution and retrieval.

REFERENCES

[1]. Junbeom Hur and Kyungtae Kang, Member, IEEE, ACM "Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks" IEEE Transaction On Networking, VOL. 22, NO.1, 2014.

[2]. 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.

[3]. Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma, and Zhenfeng Zhang "Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme" IEEE Transaction on parallel and distributed systems VOL. 24, NO. 11, November 2013

[4]. Junbeom Hur "Improving Security and Efficiency In Attribute-Based Data Sharing" IEEE Transaction On Knowlwdge and Data Engineering VOL. 25, NO. 10, October 2013

[5]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323

[6]. N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective group broadcast in vehicular networks using dynamic attribute based encryption," in Proc. Ad Hoc Netw. Workshop, 2010, pp. 1–8.

[7]. Luan Ibraimi, Qiang Tang, Pieter Hartel "Efficient and Provable Secure Ciphertext-Policy Attribute-Based Encryption Schemes", in Proc. ASI ACCS, 2009, pp. 343–352.

[8]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proc. ASI ACCS, 2010, pp. 261–270.

[9]. M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption," in Proc. ACM Conf. Comput. Commun. Security, 2009, pp. 121–130.

[10]. S. S.M. Chow, "Removing escrow from identity-based encryption," in Proc. PKC, 2009, LNCS 5443, pp. 256–276.

[11]. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attributebased systems," in Proc. ACMConf. Comput. Commun. Security, 2006, pp. 99–112.

[12]. Junbeom Hur and Dong Kun Noh, Member, IEEE "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems" IEEE Transaction On Parallel and Distributed Systems, VOL. 22, NO.7, July 2011.

[13]. Christopher N. Ververidis and George C. Polyzos "Extended ZRP: a Routing Layer Based Service Discovery Protocol for Mobile Ad Hoc Networks" in proc. IEE Conf, Networking and Services. 2005, pp. 65-72.

[14]. Tao Chen, Member, IEEE, Zheng Yang, Member, IEEE, Yunhao Liu, Senior Member, IEEE, Deke Guo, Member, IEEE, and Xueshan Luo "Localization-Oriented Network Adjustment in Wireless Ad Hoc and Sensor Network.