A Novel Cipher Text Policy Attribute Based Encryption Algorithm for a Secure Data Retrieval in Military Networks

Vema Lakshmi Prasanna [#1], CH. K. Rupesh Kumar [*2]
*M.Tech Scholar [#1], Assistant Professor [*2]*
Department of Computer Science & Engineering,
Vizag Institute of Technology, Dakamarri, Bheemili (M),
Visakhapatnam-531162, AP, India

Abstract: **Now a day's wireless sensor networks have achieved maximum user attention towards their usage. Mobile Adhoc Networks are the devices which are always self-configuration nodes connected without any wires. Generally in manets each and every device has a chance to move from one location to other location independently without having any restriction. Almost all military officials use Manets as main source or medium in order to have communication at the time of battlefields or hostile regions. As this Manets are used by lot of military officials, still there were some problems that arise while using Manets like intermittent network connectivity and frequent network partitions. To avoid the problem of intermittent network connectivity, almost each and every military official are preferred with a new type of network called as Disruption Tolerant Network (DTN). By using this DTN, the soldiers can communicate with each other and access the confidential data or commands without having any intervention between their communication.Eventhough a lot of mobile users are taking DTN technology as advantage they still face some challenging issues like authorization and secure data retrieval. Inorder to solve this challenging issues we use an advanced cryptography algorithm like Attribute Based Encryption with Cipher Text Policy. Also we have used the Identity Based Encryption algorithm in order to encrypt the data which is stored in storage node by the sender and here we use secret key encryption for generating the keys dynamically by the server. By conducting various experiments on this proposed ABE over Cipher text policy on Military networks we finally came to a conclusion that this proposed system is more secure in keeping data confidentially in the disruption-tolerant military network.**

***Keywords*: Attribute Based Encryption, Adhoc Networks, Encryption, Cipher text Policy.**

1. Introduction

In current days there was a lot of development in electronic technology, which laid the way for the development of a new generation of wireless sensor networks (WSNs) consisting of a large number of low-power, low-cost sensor nodes that communicate remotely [1]. Such sensor networks can be used in a wide range of applications, such as, military sensing and tracking, health monitoring, data acquisition in hazardous environments and habitat monitors [2]. The sensed data often need to be sent back to the base station for analysis. However, when the sensing field is too far from the base station, transmitting the data over long distances using multihop may weaken the security strength and increasing the energy consumption at nodes near the base station, reducing the lifetime of the network. Therefore, mobile sinks (MSs) (or mobile soldiers, mobile sensor nodes) are essential components in the operation of many sensor

network applications, including data collection in hazardous environments, localized reprogramming, oceanographic data collection, and military navigation [8]- [11].

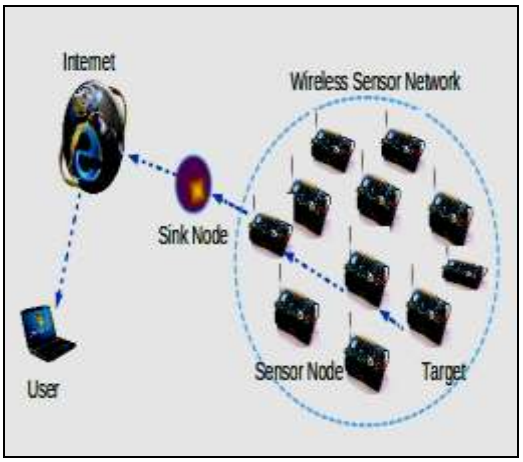

Figure 1. Represents a primitive and most popular Wireless Sensor Network

From the figure 1, we can clearly get an idea about the typical wireless sensor networks which consists of a set of sensor nodes with in a region and a sink node which is connected in order to carry the information from the user node to the target node with the internet. Generally in the wsn applications almost sensor nodes transmit critical information over the network; therefore, security services, such as, authentication and pair wise key establishment between sensor nodes and mobile sinks, are important. However, the resource constraints of the sensors and their nature of communication over a wireless medium make data confidentiality and integrity a nontrivial task. Traditional schemes in ad hoc networks using asymmetric keys are expensive due of their storage and computation cost. These limitations make key pre-distribution schemes the tools of choice to provide low cost, secure communication between sensor nodes and mobile sinks.

Disruption-tolerant network (DTN) nodes are those which are presently providing undefeated solutions that permit nodes to speak with every other in these hostile environments. Typically, when there is no end-to-end association between a source and destination nodes, then the messages from the source or supply node could need to wait within the intermediate nodes for a considerable quantity of time till the association would be eventually established. Several military [1]-[5] applications need inflated protection of confidential knowledge together with access management ways that area unit cryptographically enforced [6], [7].

Generally in the military networks there will be a key authority in order to maintain the access policy of each and every user individually. Here the key authorities are de-centralized as there will be individual key-authorities for accessing each and every functionality of military networks. For example, in a disruption-tolerant military network, a commander/officer could store sensitive information at a storage node that would be accessed by members of individual Battalion, as the data is stored in storage node the key authority should verify the identity of soldier who wants to access the data which is kept for an individual battalion. If the key authority gives access permission for that appropriate soldier from an individual battalion then he can access the data, if not the soldier cant able to access the data. During this transmission if any invalid user try to access the data of different battalion or region by him from his region, it can't be decrypted and visible for him. So he will be treated as intruder by the storage node that monitors all the user activities [10].

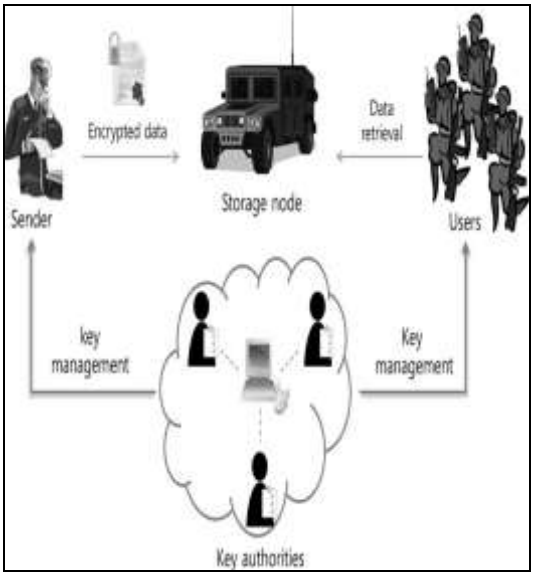

Figure. 2. Shows the Proposed Secure Data Retrieval in a DTN Network.

From the above figure 2, we can clearly found that there are various roles like sender, users, key authorities and storage node ,where the sender is a person also known as officer or commander who try to send the information or message to the soldiers who are present in different regions. The message which is given by the sender will be initially encrypted and then stored in the storage node which is the repository for all the sensitive information. Here users are nothing but soldiers who will be moving from one place to another and they will access the information from the commander. Here there is another important role like key authorities where each and every key authority acts like decentralized manner in accessing the roles for each and every soldier individually.

2. Related Work

In this section we will find the related work that was carried out in order to implement this current paper. Now let us look about the literature that was carried out on this proposed paper in detail.

A) ABE- Algorithm

Here in this section we will describe the working nature of Attribute Based Encryption (ABE) algorithm for encrypting the data at storage node. Attribute-based coding permits every ciphertext to be related to associate degree attribute, and also for the master-secret key holder, who wish to extract a secret key for a policy of those attributes. Once the attributes are substituted a ciphertext may be decrypted by this key if its associated attribute conforms to the policy. However, one of the main reason in using ABE algorithm is collusion resistance however not the compactness of secret keys. Indeed, the scale of the key usually will increase linearly with the quantity of attributes it encompasses, or the ciphertext-size isn't constant. Generally the ABE comes in 2 flavors: One is CP-ABE (Ciphertext Policy ABE) and other is: KP-ABE (Key Policy ABE).In the existing system we try to use Key Based ABE. But in this proposed paper we use CP-ABE as major algorithm for encrypting and data storing in the storage node.

1. Key-Policy ABE
2. Cipher Policy ABE

KP-ABE is that the twin to CP-ABE within the sense that Associate in Nursing access policy is encoded into the users secret key, and a ciphertext is computed with relevance a group of attributes, e.g., During this example the user wouldn't be able to decode the ciphertext however would for example be able to decode a ciphertext with relevance .An important property that needs to be achieved by each, CP-ABE and KP-ABE is named collusion resistance. This primarily implies that it mustn't be potential for distinct users to "pool" their secret keys specified may along decode a ciphertext that neither of them could decode on

their own (which is achieved by severally randomizing users' secret keys).

3. A Novel CP-ABE Algorithm

In this section, we describe a novel multi authority ciphertext policy attribute based encryption algorithm for secure data retrieval in a decentralized DTN.

A) Main Motivation

In this section we will discuss about the assumptions that were used in order to store and retrieve the data in a secure manner in a disruption tolerant military networks. Each local authority issues partial personalized and attribute key components to a user by performing secure 2PC protocol with the central authority. Each attribute key of a user can be updated individually and immediately. Thus, the scalability and security can be enhanced in the proposed scheme.

Since the primary CP-ABE theme projected by Bethencourt et al. [13], dozens of CP-ABE schemes have been projected [7], [12]–[14]. The next CP-ABE schemes are a unit principally motivated by a lot of rigorous security proof in the normal model. However, most of the schemes didn't achieve the quality of the Bethencourt et al.'s scheme, which delineated associate degree economical system that was communicatory in that it allowed associate degree encrypt or to specific associate degree access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we have a tendency to develop a variation of the CP-ABE rule partially supported (but not restricted to) Bethencourt et al.'s construction so as to reinforce the quality of the access management policy rather than building a brand new CP-ABE scheme from scratch.

B) Scheme Construction

In this section we will describe the attributes that are required for constructing the proposed scheme. Now let us discuss about them in a brief.

i) System Setup Attribute

In the initial system setup phase, the trusted initializer chooses a bilinear group G_0 of prime order with generator according to the security parameter. It also chooses hash functions

$$H : \{0,1\}^* \rightarrow \mathbb{G}_0$$

From a family of universal one-way hash functions. The public parameter *param* is given by (G_0, g, H). For brevity, the public parameter *param* is omitted below.

ii) Central Key Authority Attribute

CKA chooses a random exponent $\beta \varepsilon R Z_p^*$. It sets $h=g^{\beta}$. The master public/private key pair is given by

$$(\mathrm{PK_{CA}} = h, \mathrm{MK_{CA}} = \beta).$$

Local Key Authorities: Each chooses a random exponent $\alpha \varepsilon R Z_p^*$. The master public/private key pair is given by

$$(\mathrm{PK}_{A_i} = e(g,g)^{\alpha_i}, \mathrm{MK}_{A_i} = \alpha_i).$$

In the below section we will mainly describe the key generation module.

iii) Key Generation Attribute

In CP-ABE, user secret key parts include one personalised key and multiple attribute keys. The personalised secret is unambiguously determined for every user to stop collusion attack among users with completely different attributes. The projected key generation protocol consists of the non-public key generation followed by the attribute key

generation protocols. It exploits arithmetic secure 2PC protocol to eliminate the key written agreement downside such none of the authorities will verify the entire key parts of users separately.

4. Implementation Modules

Implementation is the stage where the theoretical design is turned out to be to practical manner. Generally the implementation stage is used for dividing the application into a set of modules uniquely. In this paper we have divided into 5 modules in order to show the performance of this proposed application. Now let's look at each module in detail.

A. Sender Module
B. DTN Router Module
C. Key Authority Module
D. End User Module
E. Threat Identification Module

A. Sender Module

In this module, the Sender is responsible for registering the Users by providing details Name, Password, Confirm Password, Battalion (b1,b2,b3) , Region(R1,R2,R3). Sender Browses the data File, encrypts it and gets the key from Key Authority Server (KA1, KA2, and KA3). Uploads their data files to the Storage Node and sender is authenticated to provide privileges for End User.

B. DTN Router Module

The Disruption Tolerant Network Router (DTN) technologies are becoming successful solutions in military applications that allow wireless devices to communicate with each other and access the confidential information reliably by exploiting external storage nodes. In this module we introduced storage nodes in DTNs where data is stored or replicated such that only authorized mobile nodes can access the necessary information quickly and efficiently. In DTN encrypted data file and details will be stored in Storage Node.

C. Key Authority Module

The key authority (KA1, KA2, and KA3) is responsible to generate the secret key for the file belongs to the particular Battalion and region. The End User Request to the storage node using the file Name, secret key, Battalion and Region, Then storage node connect to the respective Key authority server. If all specified Details are correct then file will sent to the end user, or else he will be blocked in a storage node. The Key Authority server can view the users, privileges, keys. Thus, the key authority can decrypt every cipher text addressed to specific users by generating their attribute keys.

D. End User Module

In this module, the End user can access the file details and end user who will request and gets file contents response from the DTN Router. If the credential file name and secret key is correct then the end user will get the file response from the router in Decrypted format.

E. Threat Model Module

Threat model is one who is trying to access the file which is belongs to other user by injecting the fake details to the file in the storage node is considered as Attacker. The attacker can be Data confidentiality or collusion-resistance.

i) **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.

ii) **Collusion-resistance:** Suppose there exist a user with attributes {"Battalion 1", "Region 1"} and another user with

attributes {"Battalion 2", "Region 2"}. They may succeed in decrypting a cipher text encrypted under the access policy of ("Battalion 1" AND "Region 2"), even if each of them cannot decrypt it individually. We do not want these colluders to be able to decrypt the secret information by combining their attributes. We also consider collusion attack among curious local authorities to derive user's keys.

5. Conclusion

In this paper we finally have used DTN networks as major source for secure data storage and retrieval in the military networks. By using this DTN networks, the soldiers can communicate with each other and access the confidential data or commands without having any third party intervention between their communications. As we know that there were a lot of mobile users who is taking DTN technology as an advantage they still face some challenging issues like authorization and secure data retrieval. SO in this paper we have implemented a novel algorithm like Attribute Based Encryption with Cipher Text Policy. As an extension we have implemented the Simulation results on Network Simulator tool which was mainly designed in java to show the performance of DTN over military networks.

References

[1] Y. Tirta, Z. Li, Y. Lu, and S. Bagchi, "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc. 13th Int'l Conf. Computer Comm. and Networks (ICCCN '04), Oct.2004.

[2] H. Chan, A. Perrig, and D. Song, "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303, Kluwer Academic, 2004.

[3] A. Rasheed and R. Mahapatra, "An Efficient Key Distribution Scheme for Establishing Pairwise Keys with a Mobile Sink in Distributed Sensor Networks," Proc. IEEE 27th Int'l Performance Computing and Comm. Conf. (IPCCC '08), pp. 264-270, Dec. 2008.

[4] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to-Peer Systems (IPTPS '02), Mar. 2002.

[5] H. Deng, W. Li, and D.P. Agrawal, "Routing Security in Wireless Ad Hoc Networks," Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[6] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," Proc. MobiCom, pp. 56-67, 2000.

[7] D. Huang and M. Verma, "ASPE: Attribute-based secure policy social control in conveyance impromptu networks," impromptu Netw., vol. 7, no. 8, pp. 1526–1535, 2009.

[8] S. Roy andM. Chuah, "Secure knowledge retrieval supported ciphertext policy attribute-based encoding (CP-ABE) system for the DTNs," Lehigh CSE Tech. Rep., 2009.

[9] A. Lewko and B. Waters, "Decentralizing attribute-based encoding," Cryptology ePrint Archive: Rep. 2010/351, 2010.

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

[11] M. Chuah and P. Yang, "Node density-based accommodative routing theme for disruption tolerant networks," in Proc. IEEE MILCOM, 2006, pp. 1–6.

[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: ascendible secure file sharing on untrusted storage," in Proc. Conf. File Storage Technol., 2003, pp. 29–42.

[13] M. Chuah and P. Yang, "Performance analysis of content-based information retrieval schemes for DTNs," in Proc. IEEE MILCOM, 2007, pp. 1–7.

[14] N. Chen, M. Gerla, D. Huang, and X. Hong, "Secure, selective cluster broadcast in conveyance networks victimization dynamic attribute based mostly encoding," in Proc. impromptu Netw. Workshop, 2010, pp. 1–8.

About the Authors

VEMA LAKSHMI PRASANNA is currently pursuing her 2 Years M.Tech in Computer Science and Engineering at Vizag Institute of Technology, Dakamarri, Bheemili (M), Visakhapatnam, AP, India. Her area of interests includes Java, Computer Networks.

CH. K. RUPESH KUMAR is currently working as Assistant Professor in Department of Computer Science and Engineering at Vizag Institute of Technology, Dakamarri, Bheemili (M), Visakhapatnam, AP, and India.He has a total of 3 years of experience in teaching field. His research interest includes Computer Networks and Artificial Intelligence.

