ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Secret Key Issuing for Decentralized Disruption Tolerant Networks Using Partial Key Distribution

N.Asha Latha, CH.V.Sarma

PG Scholar, Dept. of C.S.E., Vignan's Institute of Information Technology, Visakhapatnam, India

Sr. Assistant Professor, Dept. of C.S.E., Vignan's Institute of Information Technology, Visakhapatnam, India

ABSTRACT: Disruption-tolerant networks (DTN's) are successful solutions when there are connectivity issues (intermittent connectivity, Long or Variable Delay, Asymmetric Data Rates, High Error Rates) in the network. DTN's are wireless networks. DTN's provide external storage nodes in the network. Confidential information is stored in these storage nodes when there is communication problem in the network among the users in the network. In hostile environments storing and retrieving of data from these storage nodes becomes complicated. Cipher text-policy attribute-based encryption (CP-ABE) is a cryptographic solution to access control issues in DTN's. For secure data retrieval from these storage nodes CP-ABE scheme is used. While applying CP-ABE in decentralized DTNs introduces several security and privacy challenges with regard to the attribute revocation, key escrow, and coordination of attributes issued from different authorities. In this paper we propose a scheme known as Partial key Distribution for DTN's for securing the secret keys and confidential data. Here we will explain how the Partial key distribution scheme protects the confidentiality of data.

KEYWORDS: Attribute revocation, Cipher text-policy attribute-based encryption (CP-ABE), Disruption-tolerant networks (DTN's), key escrow, Partial key Distribution.

I. INTRODUCTION

When mobile nodes operate in hostile environments, communication is disrupted by jamming, environmental factors and mobility. DTN's are successful solutions when there are connectivity issues (intermittent connectivity, Long or Variable Delay, Asymmetric Data Rates, High Error Rates) in the network. When there is no direct communication between source and destination pair, the messages from source node waits at intermediate nodes (storage nodes) until the connection is established. These storage nodes are introduced by Roy [2] and Chuah [3].

The information stored in storage nodes is only accessed by authorized mobile nodes. To provide confidentiality of information crypto graphical methods are used. Sometimes it might be required to provide access policies that are managed by key authorities.

Attribute based encryption [4]–[7] is a method for secure data retrieval in DTN's. It facilitates the access control over encrypted data using credited attributes and access policies among cipher texts and private keys. In CP-ABE encryptor defines the attribute set that the decryptor needs to acquire to decrypt the cipher text [6]. While applying ABE to DTN's there are several security and privacy issues. Some users may change their associated attributes at some point, or some private keys might be compromised, key revocation for each attribute is necessary in order to make the system secure. In ABE the revocation of any attribute in an attribute group would affect the others. For example if any user leaves or joins the attribute group, the associated attribute key should be changed and redistributed to all other members of the group for forward and backward secrecy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Another problem with CP-ABE scheme is key escrow problem. Key authority generates private keys of users by applying the authority's master secret key to user's associated set of attributes. The key authority can decrypt every cipher text. This could become a threat to data confidentiality when the data is sensitive. In multiple-authorities systems as each key authority generates its own attribute keys with their own master keys then key escrow problem arises. When multiple authorities manage their attributes independently with their own master secret keys, it is difficult to define access policies over attributes issued by different authorities.

II. RELATED WORK

ABE has two types called key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In KP-ABE, the key authority defines access policy and embeds it into the key and sends it to decryptor. In CP-ABE, the ciphertext is encrypted with an access policy chosen by an encryptor, but a key is created with attributes set. CP-ABE is more appropriate to DTNs than KP-ABE because it enables encryptors to choose an access policy on attributes and to encrypt confidential data.

1) Attribute Revocation: When a user wants to move from one location to another then their attributes change according to their location. For example when we travel to other country we change our mobile numbers. So when the user moves to other location they will revoke their attributes. These revocation mechanisms are first introduced by Bethencourt *et al.* [6] and Boldyreva *et al.* [8]. They suggested periodic rekeying mechanisms. It creates a problem in terms of Forward and Backward secrecy. To overcome that CP-ABE mechanism is used. In CP-ABE the key is derived from the attributes of multiple users and distributed to them. When one user revokes their attribute then the key must be changed with new attributes of remained users. If the key is not changed then the revoked user can decrypt the confidential messages sent to that user group (forward secrecy). The revoked user can decrypt the previous messages addressed to different users with that key (backward secrecy). So the new key should be re distributed to all the users. Re distribution after every revocation creates a scalability problem. To overcome these problems a Secure CP-ABE [1] scheme is proposed. In this scheme forward and backward secrecy are achieved by reducing the windows of vulnerability. If the system or user is in hostile environment then forward or backward secrecy is not guaranteed.

2) Key Escrow: In many ABE schemes one central key authority generates the user's private keys using authority's master secret key [4], [6], [7], [9]–[11]. Whereas the key authority can decrypt every cipher text addressed to users. To overcome this problem multi authority system [12] is proposed. In multi authority system all individual authorities participate with their attributes. It is difficult to gain the possibilities of that key. But the problem arises when the authorities fail to communicate with each other resulting performance degradation in the system. In secure CP-ABE scheme they proposed an access tree structure. If the parent node fails in the access tree then it is impossible to calculate ϒ values and is difficult to calculate key and encryption and decryption [1].

3) Multi authority System: Decentralized ABE scheme is proposed in multi authority environment by Huang *et al.* [9]. When multiple authorities participate, it is difficult to generate a combined access policy. It has done by encrypting the data multiple times. But it is not efficient. While decrypting there will be mystification because of there is no expressiveness in the policy.

III.CONTRIBUTION

In this paper we propose partial key distribution approach for decentralized DTN's. The proposed scheme overcomes the above problems. It overcomes the attribute revocation problem by distributing secret key to partial key authorities. Key Escrow problem will be solved as CKA does not know the access policy of the sender or receiver. To decrypt the cipher text there is no necessity to consider all the authorities in the network so multi authority system problem will be solved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

IV. NETWORK ARCHITECTURE

In this section, we designed DTN architecture. First we start with describing the entities in the system. After that we describe the security requirements of the system.

A. Entities and Assumptions

The system consists of the following entities.

1) Central Key Authority (CKA): It works as key generation center. It authenticates every user and generates an id and master secret key. It divides the master secret key into parts and those partial keys are distributed to partial key authorities. We assume CKA has been highly fault tolerant and always available.

2) Partial Key Authority (PKA): There are n partial key authorities in every network. These authorities are nothing but the other nodes in that network. They are designed to provide privacy to the partial key. These authorities provide partial keys to users when authenticated users requests for partial key. These are not as reliable as CKA. To authenticate PKA's Byzantine fault tolerance protocol [10] is used.

3) Storage Node (SN): When there is no proper communication between sender and receiver then the data is stored in these storage nodes. Only encrypted data will be stored in these nodes for providing confidentiality. Receiver contacts this storage node when he lost communication with sender while sender stores the message and receiver's information in these nodes. We assume it has been highly fault tolerant and always available.

4) Sender: This is a user who owns the confidential data and desires to store them into external storage node for reliable delivery to users in hostile environments. Sender is responsible for choosing an access policy and for encrypting the data before storing it to the storage node.

5) Users: This is a node in the network who wants access the stored data from the storage node. If the user satisfies the requirements of the sender then he will be able to decrypt the cipher text and to access the original data.

Fig .1.,

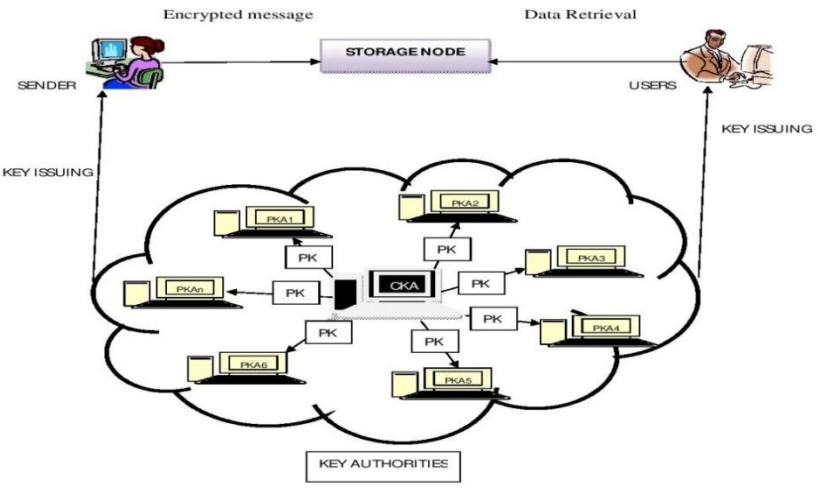

FIG: ARCHITECTURE OF PARTIAL KEY DISTRIBUTION FOR DISRUPTION TOLERANT NETWORKS

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

B. Security Requirements

1) Data confidentiality: Unauthorized users should be deterred from accessing the data in the storage node. Unauthorized access from the storage node or key authorities should also be prevented.

2) Backward and forward Secrecy: Revoked users should not be able to access the subsequent data after revocation. New user should not be able to access the plain text exchanged before his arrival.

3) Secure key issuing: It must provide a method for secure key issuing when there is no secure channel, and defend against the attacks in the network.

V. PROPOSED SCHEME

Here we provide a partial key distribution scheme for secure key issuing in decentralized DTN's. There are one CKA and n PKA nodes at the setup phase. First, CKA selects a master key, publishes its identity (ID) [8] [14] and specifies the system parameters. Next CKA assigns to each PKA node an ID and a corresponding private key based on IBC scheme via a secure offline channel. This is only required at the system setup phase.

1) Node Registration: If a node wishes to enter into a network then it should get registered with CKA. When a node sends a request to CKA, CKA generates a unique ID and secret key for that node and sends ID to the node and secret key to the PKA's. Assigning ID by CKA prevents the node from choosing its own ID. CKA can be discovered by automatic service mechanism. While sending a request to CKA node adds a Nonce N to the request to avoid replay attacks. This nonce can be used to verify the sender after key generation.

The protocol is specified as follows.

NODE ⟶ CKA : Request, N
CKA ⟶ NODE : ID, N
CKA ⟶ PKA's : SS (SK, k), N

To avoid man-in-the-middle attacks CKA generates a message digest of node's ID and sends it with ID. Node cross checks it by again calculating the message digest of the ID and compares it with the received message digest. If both are same then no change in the node's ID, it would continue with its operations.

2) Partial Key Distribution: After assigning ID to node CKA generates a secret key for that node. CKA divides the secret into secret shares (partial keys) and sends them to n PKA's. The generation of the partial keys is done using Shamir's (k, n) threshold Secret Sharing scheme [13][15].

A) Shamir's (k, n) threshold Secret Sharing Algorithm:

If we want to use (k, n) threshold scheme to share our secret S where $k < n$.

I. Choose at random (k-1) coefficients $a_1, a_2, a_3 \ldots . a_{k-1}$

II. Choose $a_0 =$ Secret S (i.e., in our algorithm S is our secret key)

III. Construct the polynomial of degree k-1. This polynomial is constructed over a finite field.
$f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots\ldots\ldots + a_{k-1} x^{k-1}$

IV. Choose n random distinct evaluation points $x_i ! = 0$ and construct n points (i ,f (i)) where i=1, 2, 3, ……, n.

V. Distribute these distinct values to PKA's. The distinct f(i) values are the partial keys.

3) Secret Key Reconstruction: Reconstruction of secret key is only done when there are at least k partial keys. Even k-1 partial keys cannot reconstruct the secret key. This reconstruction is done by using Lagrange Interpolation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

B) Reconstruction Algorithm:

I. Node sends a request to k PKA's using its ID.
II. PKA's authenticates it and provides their partial keys.
III. To find the polynomial f(x) gather at least k partial keys from k PKA's.
IV. Calculate Lagrange's polynomials
$L_i(X) = \prod_{j \neq i}(x - xj) / \prod_{j \neq i}(x\,i - xj)$
V. Calculate the final polynomial using
$F(X) = \sum_{i=1}^{k} f(i) \times Li(x)$

4) Encryption: Secret key is reconstructed from k partial keys. Only authenticated users can get those partial keys. This secret key is used to encrypt the messages send by the sender. Encrypted messages are stored in external storage node and if the receiver is currently available then the messages are also delivered to the receiver. Encryption of the messages is done by using Advanced Encryption Standard algorithm.
Advanced Encryption Standard (AES) Algorithm:

1. Derive the set of round keys from the derived secret key.
2. Initialize the state array with the block data (Plain text).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final rounds of manipulation.

Copy the final state array output as the encrypted data (cipher text). Store the encrypted data into storage node if the receiver is unavailable. If the receiver is available then directly send the data.

5) Decryption: If the receiver is currently available in the network then he will get the message directly. He will request k KPA's for partial keys and then reconstructs the secret key for decrypting the message. If the receiver is not present then he will check in the storage node for messages. If any messages available then he will decrypt the data using the secret key. This secret key reconstructed from the k partial keys.

VI. SECURITY

The nodes which are not registered with CKA cannot get in contact with Storage Node. They cannot send or receive messages from registered nodes. Unauthorized users have no access to the data without proper registration data. Even if the attacker knows the nodes id he will be denied by PKA's while authentication. PKA's cannot access the data because they don't know the secret key. Even if k authorities tries to cooperate with each other they cannot get the secret key as they don't have the reconstruction algorithm there by data confidentiality is maintained.

The users who are revoked cannot access the next data after revocation because CKA completely removes the revoked user's data. There by forward secrecy is maintained. The revoked user cannot decrypt the previous data after revocation because CKA removes all the data access with that user's secret key. There by backward secrecy is maintained.

Even though there is no security in the network the secret key is distributed to PKA's as partial keys. Those partial keys are reconstructed by user for encryption and decryption of the data to store or retrieve from the Storage node. There by security is maintained while key issuing and retrieving phases.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

VII. RESULTS

CKA: It generates an ID and secret key for users. It divides the secret key into k partial keys and sends them to PKA's. Each partial key is sent to respected partial key authorities.

Fig 2: key generation by Central Key Authority.

NODE: Every node in the network should have to register with CKA. CKA generates an ID for each node. The node registration is shown below.

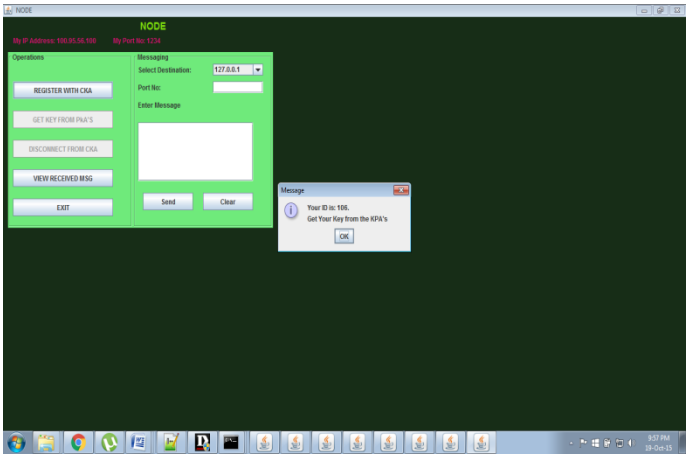

Fig 3: Registration of a node with CKA

Sending and Retrieving messages: After sending a message to receiver based on its identity a message will be displayed on the sender window for successful sending of the messages. At the receiver window sender details are displayed when the receiver is available. Then the receiver contacts the PKA's for secret key reconstruction. Figure 4 shows the successful message displayed on the sender window. Figure 5 shows the receiver's window message after successful receiving of the message. Figure 6,7 shows retrieving messages from kpa's. There by messages are successfully retrieved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

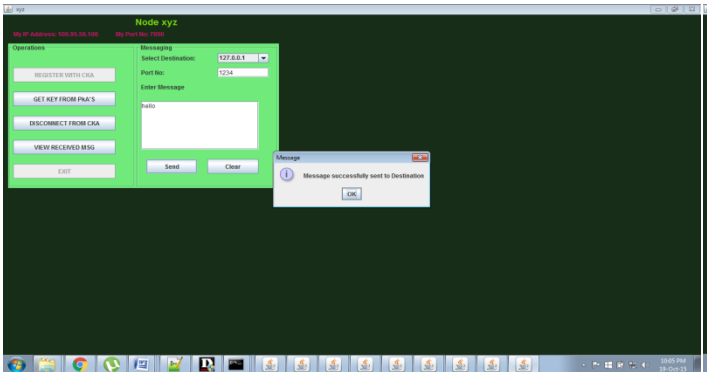

Fig 4: sending of message at sender window

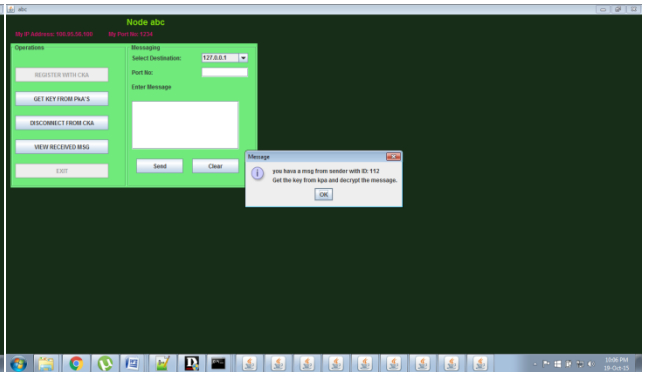

Fig 5: successful receiving at receiver's window

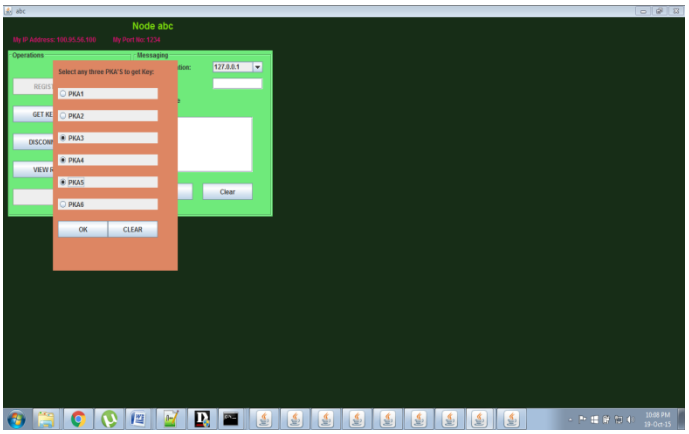

Fig 6: Selecting k PKA's

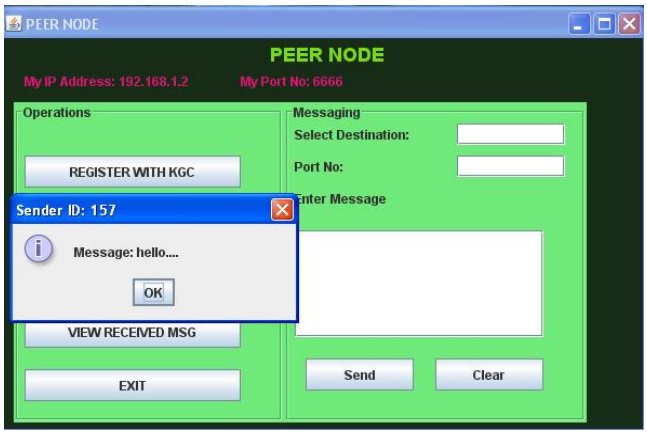

Fig 7: Displayed message at receiver's window

VIII. CONCLUSION

In this paper the proposed scheme solves the attribute revocation and key escrow problems. Forward and backward secrecy of the data is also provided. PKA's are authenticated by using byzantine fault tolerance protocol. Cooperation between the key authorities to get secret key is denied. The proposed scheme avoids multiple encryptions of the data and provides an efficient access policy for the users. The proposed scheme avoids the loss of the data by exploring the external storage nodes in the network. There by data integrity is provided. Our scheme solves the specified problems (key escrow, attribute revocation, backward and forward secrecy of the data) and provides an effective and efficient access policy to users.

REFERENCES

[1] Junbeom Hur and Kyungtae Kang., "Secure Data Retrieval for Decentralized Disruption- Tolerant Military Networks", IEEE Transactions on Networking, vol. 22 no: 1 year 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] M. Chuah and P. Yang, "Performance evaluation of content-based information retrieval schemes for DTNs", in Proc. IEEE MILCOM, pp. 1–7, 2007.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption", in *Proc. Eurocrypt*, pp. 457–473, 2005.
[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", in Proc. ACM

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 10, October 2015

Conf. Comput. Commun. Security, pp. 89–98,2006.
[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption", in Proc. IEEE Symp. Security Privacy, pp. 321–334, 2007.
[7] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures", in Proc. ACM Conf. Comput. Commun. Security, pp. 195–203,2007.
[8] A.Boldyreva, V.Goyal, and V. Kumar, "Identity-based encryption with efficient revocation", in Proc. ACM Conf. Comput. Commun. Security, pp. 417–426,2008.
[9] L. Cheung and C. Newport, "Provably secure ciphertext policy ABE", in Proc. ACM Conf. Comput. Commun. Security, pp. 456–465,2007.
[10] V.Goyal, A. Jain,O. Pandey, andA. Sahai, "Bounded ciphertext policy attribute-based encryption", in Proc. ICALP, pp. 579–591, 2008.
[11] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption", in Proc. ASIACCS, pp. 343–352,2009.
[12] M. Chase and S. S. M. Chow, "Improving privacy and security in multiauthority attribute-based encryption", in Proc. ACM Conf. Comput. Commun. Security, pp. 121–130,2009.
[13] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.
[14] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO, pp. 47–53,1984.
[15] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in id-based cryptography", in ACSW Frontiers, pp. 69–74, 2004.

BIOGRAPHY

N. Asha Latha is a PG scholor in computer science and engineering Department, Vignan's Institute of Information Technology, Visakhapatnam, India. She received her Bachelor degree in 2013. Her research interests are Computer Networks (wireless Networks), Algorithms. etc.

CH.V.Sarma is a Senior Assistant Professor in computer science and engineering Department, Vignan's Institute of Information Technology, Visakhapatnam, India. He received his MSc degree in 2002. He received his M.Tech degree in 2009. His research interests are Artificial Intelligence, Neural networks, Computer Networks etc.