Privacy Preserving Task Force Communication in Hastily Formed Networks through ACT

Biji Nair[1]*, M. Sridevi[1], C. Mala[1], and Lakshmi Prabha S[2]
[1]Department of Computer Science and Engineering
National Institute of Technology Trichy, Tamil Nadu, India
nairbiji@rediffmail.com, {msridevi, mala}@nitt.edu
[2]Department of Computer Application
National Institute of Technology Trichy, Tamil Nadu, India
jaislp3@gmail.com

Abstract

Task Forces are groups formed to command, control and manage time bound emergency situations like rescue and relief operations, event management, emergency health care assistance, through collaborative effort. Technological assistance and coordination among the members of the Task Forces are critical for accomplishing their mission. The proposed work gives a scheme for secure and privacy preserving group communication among the members at different hierarchical levels of the Task Force. Mostly such tasks are to be carried out in conditions of scarce infrastructural availability. Communication among the members of the Task Force is based on their responsibility and authority within the sub-group to which they belong and can be realized through Mobile Adhoc Network (MANET). The proposed system achieves privacy and security in communication through Access Control Tree (ACT) structure using Ciphertext Policy Attribute Based Encryption (CP-ABE). The proposed solution supports two essential requirements of a Task Force for accomplishing its goal within the stipulated time. One, a well organized Task Force with clear division of responsibility and authority and the other, secure and privacy retaining communication among the members of the group.

Keywords: Privacy, Security, Ciphertext Policy Attribute Based Encryption, secure group communication, MANET, Access Control Tree

1 Introduction

Task Forces are formed with an aim of accomplishing a project or a mission within a short span of time. Since these groups are formed for a purpose, they are temporary in nature and exist till the accomplishment of the task. Task Forces include work teams, rescue operators, event managers and also informal committees. Task Forces may be formed on short notice and also of people unknown to each other. Each member of the group is assigned distinct responsibility and authority. Formation and smooth operation of such groups require communication devices and secure medium of communication among the group. The proposed work is a solution for group communication among members of a Task Force formed for specific and result oriented operations like event management, meetings, conferences, health care monitoring or relief and rescue operation. Temporary Adhoc networks are a boon for applications where there is a requirement of spontaneous setup of self-dependent networks, in places with limited or no availability of infrastructure. Such networks are called Hastily Formed Networks (HFN). Mobile Adhoc Networks (MANET) are self organizing, self-configuring networks formed from mobile devices

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 2, Article No. 6 (August 31, 2016)
*Corresponding author: Department of of Computer Science and Engineering, National Institute of Technology, Trichy, Tamil Nadu, 620015, India, Tel: +81-294-38-5138

connected through wireless communication. MANET [3] is the technological solution for connectivity in applications like natural disaster, emergency health care requirements, warfare and in human-hazardous environments. The requirement of these applications, is not just connectivity, but also security and privacy preserving communication of information. The Task Force members are connected to each other through MANET that offers free mobility (within range) and connectivity for their progress in their task. The type of communication essentially required, among the members of the group are point-to-point, broadcast and multicast with privacy and security. The proposed solution offers privacy preserving multicast communication using the concept of Ciphertext-Policy Attribute-Based Encryption(CP-ABE)[4] for encrypting the messages intended for a specific set of recipients forming a sub-group. The popular encryption method of Identity Based Encryption [10] is considered an instance of Ciphertext-Policy Attribute-Based Encryption. Identity Based Encryption makes use of a single public key, and the master key is used to generate the private keys. CP-ABE is more elaborate in specifying the private keys that can decrypt a particular ciphertext. Encryption of a message is done based on an access policy and the private keys are associated to the attributes based on the access policy. Those recipients with matching set of attributes to the access policy in the ciphertext can decrypt it. This gives implicit authorization to the individuals holding the access policy.

2 Related Works

There are a lot of research done in data security in MANET as in [2], [7]. But it is not sufficient for applications requiring secure as well as privacy preserving multicast communication within the sub-groups forming the Task Force. Attribute based cryptography offers security along with privacy for multicast communication by using some features other than just the primary key of the receiver for decryption of a ciphertext. The concept of Attribute Based Encryption (ABE) was introduced by Sahai and Waters[4], but their solution were limited to specifying thresholds for access policy. Here the sender's and the receiver's private keys are associated with a set of attributes. The ciphertext will also contain the access policy that is based over the attribute set in the private keys. Decryption is possible only if a minimum of k attributes of the receiver match with the attribute set given in the ciphertext. The concept of ABE has been widely used to secure encrypted data in large storage servers, making the data secure even if the server is vulnerable. This application of ABE has been used to secure data in cloud storage[11]. They are based on fuzzy evaluation [9] of the biometric attributes of the users and was oriented towards acquiring a error-tolerant system. The demerit of [4] is that it could be applied for applications working only on fuzzy attributes. [12] proposes three constructions for specifying access control using access formula in terms of attributes of the system. The notion of multi-authority ABE using threshold ABE[8] has also been in literature, but it faces the problem of collusion attack and have not received much attention. Here adoption of a generalized access policy becomes difficult. Also the practical implementation becomes complex and cumbersome. Due to these limitation of the existing scheme the application of the above described solutions for privacy preserving group communication becomes difficult. Hence more practical implementation of Attribute Based Encryption need to be formulated so that it can suit the needs of real time applications that are time bounded.

3 Proposed Method

The existing set of privacy preserving communication solutions cannot be applied directly to the applications like group communication in Task Force operation scenario. The concept of CP-ABE is used in the proposed system named, ACT-in-HFN(Hastily Formed Networks), but with relevant modifications

to meet the requirements of the current application. The work presented here divides the problem of security and privacy preserving group communication in Task Forces into two.

1. Task Force Organization:- While forming the Task Force [5] similar to the emergency preparedness work group [1] , clear lines of authority and responsibility are defined for each members of the group. It defines the chain of command in the Task Force. Division of labor defines responsibility and the span of control decides authority. The success of operation of such Task Force demands unity of command, that is each member reports to only one superior. Proper organization of the Task Force helps achieving the specific objective of its formation, in a collaborated and coordinated manner. It also helps in optimizing technological and human resources.

2. The technology assisting the Task Force- Right networking technology is needed to help the Task Force achieve their objectives. When meager infrastructure is available in the operation area, MANET[3] is the right solution to offer mobility as well as connectivity. Along with this a hurdle free, secure and privacy retained communication service must be provided so that the Task Force can complete their operation within their time bounds. In applications demanding security and privacy preserving group communication, the proposed system offers a solution.

3.1 Task Force Organization

The Task Force is formed based on an organizational structure, where each member is assigned a subtask with clear roles and responsibilities. Also an unambiguous representation of authority and responsibility is defined using Line-and-Staff organizational structure. This particular organizational model is adopted for group formation as it offers clear line of distinction between responsibility and authority. There is no ambiguity as to who reports to whom and what one's responsibility is. Line-and-Staff organization structure is best suited for task which are time constrained and to be implemented in war footing basis.

Fig 1. shows an example of Task Force organization using Line and Staff Organization Structure. There are three types of authority defined in Line-and-Staff organization structure. They are line, staff and functional. Line Authority is the flow of chain of command. Authority gives the power of command on the individuals subordinate to him. Subordinates report to the individual above them in the line of command. Staff Authority advices line authority on its field of authority. It mostly gives important feedbacks to improve line operations. The third type of authority is the Functional Authority, and has limited authority. Group members employed for specialized task having expertise over an area are given Functional Authority. Sub-groups are formed within the Task Force with respect to each line of authority. The advantage of Line-and-Staff organization structure is that it unambiguously defines responsibility and authority, thereby making clear distinctions of sub-group formation within the Task Force. Broadcast group communication within these sub-groups is to be maintained. This facilitates flow of commands down the chain of command. Reporting is made in the reverse direction from bottom of the organizational structure to the top i.e to the authority. This type of organization of the Task Force can systematically attain the goal through command and cooperation within the stipulated time. A centralized control is maintained by the individuals holding the position of authority. Each authority forms a sub-group of his subordinates. Hence there are sub-groups formed by each node in the line of command. Once a Task Force is formed for achieving the specified task, next, the network technology for communication among the members of the group, need to be chosen.

3.2 The need for privacy in Task Force communication

A formal organization of the Task Force defines clear lines of distinction between authority and responsibility. It gives a formal line of reporting and flow of information within the Task Force. In the chain

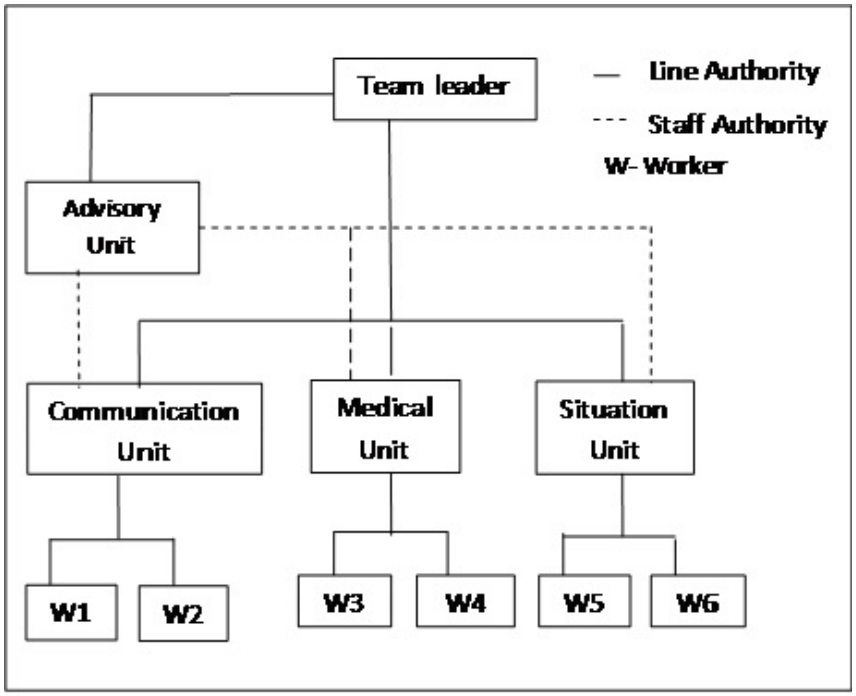

Figure 1: The sensing area is with Gaussian distributed sensor nodes

of command the superiors in the hierarchy is responsible for supervising, guiding and managing his immediate subordinates and in return subordinates report only to one superior. For this reason, a sub-group is formed among a superior and his subordinates and communication takes place within the sub-group. Hence the entire Task Force is formed of overlapping sub-groups and the communication from top of the Task Force to bottom and vice versa occurs efficiently. The communication between a superior and his subordinates to be shared beyond their group is absolutely unnecessary and at times should be preserved within the sub-group depending on the application. For example in applications such as countering terrorism and insurgency operations, warfare etc., privacy within the group is of at most importance. In case of applications like rescue and relief operations, receiving unwanted messages not relevant to the concerned individual diverts the concentration and attention of the members of the group, thereby wasting golden time to save lives. This establishes the necessity of privacy in sub-group communication thereby demanding for a solution that provides privacy preserving multicast communication.

3.3 The technology assisting the Task Force

Considering the nature of the operation of the Task Force, the most feasible and appropriate solution would be to form a Mobile Adhoc Network (MANET). Mobile devices, for instance, smart phones, used by the members of the group, can dynamically form a MANET [3], without the help of an existing network infrastructure. MANET has several multiple solutions in every aspect of networking from easy deployment, routing to maintaining the network immaterial of the kind of nodes used. Depending on the scale of operation and the number of nodes used, encrypted data is broadcasted using single hop or multiple hop mode of transmission. Fig 2 gives a view of a MANET deployment.

Figure2

Application insisting security and privacy should employ cryptographic methods for security im-

plementations. Symmetric key cryptography is not preferred for secured data exchange in such networks as key distribution becomes difficult due to highly dynamic nature of the nodes in the network. Members of the group join and leave the group as and when required and cannot be predetermined. In such a case employing symmetric key would be an added burden over the network. Public Key Cryptography is the most desirable option for data security in MANET. Though identity based public key system was first proposed by Shamir in 1984, but the practical implementation was done by Boneh and Franklin in 2001. Public key based on identity of the communicating nodes is used for cryptographic operation in Public Key Cryptography. Private Key of each node is generated and placed in the nodes before the deployment of the node in the network. The most appropriate solution is CP-ABE for ensuring security as well as privacy for the data transmission.

3.4 Ciphertext-Policy Attribute Based Encryption(CP-ABE)

Attribute Based Encryption (ABE) is an attribute based pubic key encryption method, that has the secret key or the ciphertext built on a set of attributes of the user. Ciphertext-Policy Attribute Based Encryption(CP-ABE) is a class of Attribute Based Encryption, where access control is restricted through access policy framed by the sender. The access policy over a given set of attributes is stated while encrypting the message in the ciphertext by the sender. Decryption of the ciphertext is possible if and only if the user's attributes matches the attributes endorsed in the ciphertext. This gives a mechanism for access control of the recipients by the sender, on dispersion of information. A vital strategy to mark multiple intended recipients, and avoiding others. The users are restricted based on the credentials that they should possess in order to access a given information send as ciphertext. This encryption model can be used in applications where the authorized list of users need not be known prior. Here the entry and exit of the users from the communication range cannot be predetermined. CP-ABE offers security, privacy, reliability, scalability and also some degree of anonymity to the users. But the existing solution [4] cannot be practically implemented as such for the given application, as it suffers from many disadvantages. These include, the large size the universal attribute set can attain making them difficult to handle. This also results in large overhead and high time complexity in executing encryption/decryption algorithm. Here we present the modification in CP-ABE scheme to make it feasible for implementing in the current application considered. The steps in CP-ABE algorithm is as described in [4] is given here. The key steps involved in CP-ABE algorithm are

Step 1: Setup function Setup(k) = (A, K_M)
Input - the secret key k
Output - A-The attribute set that are public parameters identifying a user
K_M - The Master Key
Setup function is used to generate the public parameters, that can generally identify all users, and the Master Key from the secret key. The Setup function is executed just once in the beginning during the set up phase of the network.

Step 2: KeyGen function $KeyGen(K_M, A) = K_A$
Input - K_M- The master Key
A- The attribute set that are public parameters identifying a user
Output - K_A-Private Key
The attributes in the set A describes the private key generated by the KeyGen function.

Step 3: Encrypt function $Encrypt(A, M, AP) = C$
Input - A-The attribute set that are public parameters identifying a user
M-Message

AP- Structure of Access Policy

Output - C -Ciphertext

Encrypt function implements the encryption algorithm. The function encrypts the message, M, and produces the Ciphertext, C, using the access policy and the public attributes so that only the users who possess the attribute in A and satisfying the access policy can decrypt the message.

Step 4: Decrypt function $Decrypt(A, C, K_A) = M$

A -The attribute set that are public parameters identifying a user

C -Ciphertext

K_A-Private Key generated for the attribute set A

Output - M -Message

Decrypt function implements the decryption algorithm. The function takes as input the attribute set A, ciphertext C, and the Private Key KA, of the user. The original message is retrieved only if the set A of attributes satisfies the access policy, AP, else the decryption algorithm suggest the message was not intended for the particular individual. The concept of Bilinear Maps defined over elliptic curve form the basis of all the above algorithms.

The access policy stated in the algorithm above is expressed as a tree form in the proposed system and is called the Access Control Tree (ACT). ACT is used to tag different encrypted data so that the Ciphertext C, generated thereafter can only be decrypted by the intended receiver. The MANET formed by the members of the group is structured as given in Fig 3. The communication within the MANET segregates it into small sub-groups containing only the authority node and its subordinate nodes. ACT contains attributes of its group only. Hence for each sub-group there is a different ACT attribute set. The structure and the concept of ACT is well described in the next section.

figure3

3.5 Access Control Trees

ACT is used to implement access control by allowing accessibility only to the intended receivers, thereby preserving privacy. Access control of the transmitted ciphertext is made possible through ACT. Here is a formal definition of ACT.

Definition of ACT : Let $S_1, S_2, \cdots, S_n$ be the number of subordinates within a sub-group. A collection of $A \subseteq 2^{S_1, S_2, \cdots, S_n}$ is monotone if $\forall B, C$: if $B \in A$ and $B \subseteq C$ then $C \in A$. An access control tree A is non empty subsets of $S_1, S_2, \cdots, S_n$ mathematically formulated as $A \subseteq 2^{S_1, S_2, \cdots, S_n}$. A is the power set of the $S_1, S_2, \cdots, S_n$, and the member sets of A is considered as Authorized sets and all others belong to Unauthorized sets. In this application $S_1, S_2, \cdots, S_n$ are the IDs of the devices of the individual members of the Task Force. Fig 4 a) gives the attribute structure of the entire Task Force. The abbreviation used in Fig 4 b) for nodes corresponds to its position in Fig 2. Each member can have many more features apart from the identification code it possess, for example the name of unit to which it belongs, the age, position held so on. The size of the public parameter increases as the number of attributes in the attribute set for each individual member increases; relatively the Universal Attribute Set also increases exponentially.

Figure5 Figure6

Large Universal Attribute set also increases the ciphertext and hence the complexity of encryption and decryption algorithm. In the proposed system Access Control structure only maintains the attribute set of the sub-group as defined in Fig4 a) and b). Hence the ID of a sub-group member is enough to identify it. Since the size of each sub-group is very small compared to the size of the Task Force, the

number of attributes in access control structure reduces relatively. This reduces the ciphertext overhead. The complexity of encryption and decryption also is less as the size of universal attributes for each sub-group is small. Fig 4. exhibits access control using access control structure.

3.6 Security Proof for CP-ABE against Chosen Plaintext Attack

Considering the nature of the operation of the Task Force, the most feasible and appropriate solution would be to form a Mobile Adhoc Network (MANET). Mobile devices, for instance, smart phones, used by the members of the group, can dynamically form a MANET [3], without the help of an existing network infrastructure. MANET has several multiple solutions in every aspect of networking from easy deployment and routing, to maintaining the network, immaterial of the kind of nodes used. Depending on the scale of operation and the number of nodes used, encrypted data is broadcasted using single hop or multiple hop mode of transmission. Fig 2 gives a view of a MANET deployment. Security against Chosen Plaintext Attack (CPA) by CP-ABE as given in [4] is briefly stated here. If an adversary A wants to compromise the security of the network he takes the help of the challenger to execute the steps of the CP-ABE algorithm as given here.

Step 1: The challenger executes the Setup function, upon receiving an access control structure A selected by an adversary. The challenger returns the public parameter A so generated, back to the adversary.

Step 2: The adversary repeatedly tries for the Private Key K_A corresponding to attribute set S, where S fails to satisfy A.

Step 3: The challenger encrypts M_t to C, $t \in 0,1$ using A. M_t is selected through flip of a random coin by the challenger from one of the two equal length messages (M_0, M_1) provided by the adversary.

(Challenge) **Step 4**: Repetition of Step1

Step 5: After executing the decryption algorithm the adversary tries to make a guess out of the messages used to check whether it is the encrypted message . A guess t' is made by the adversary out of the two values of t.

The advantage the adversary in the given game is $Pr(t' = t) - 1 \div 2$. It gives the measure of success in attacking the given cryptographic algorithm. The CPA security is reducible to Decisional Bilinear Diffie Hellman(DBDH)[6] assumption. According to [4], if every polynomial time adversary has at most a negligible advantage in the above game, then CP-ABE is secure.

3.7 Performance Analysis and Discussion

The performance of the system drastically gets improved when the number of nodes in a network gets reduced. When the Task Force is split into smaller sub-groups and each independently communicating among themselves the same algorithm of Waters[4] gets improved by logN both in size of the keys and the computational complexity.

Let us consider L_+ as the bit length of any element in $+$, T_+ the time of $+$ operations. Also, let N be the number of attributes in the system, l denotes the number of leaves in access control structure, N_s, N_s' be the size of user's attribute sets in Waters and the proposed system respectively and , I' , be the size of minimal attributes for satisfying the ACT.

For the ACT be a m-ary tree of height h , maximum number of leaves is m_h. Total number of leaves or $N = (m^{h+1} - 1) \div (m - 1)$. The maximum number of Universal attribute is terms of total number of nodes is N. But when the network is split into sub-groups as in Fig, 4b then each sub-group will

contain a maximum of m leaves i.e m attribute set. On comparing both these systems it is evident that as $m \ll N$, indicating a drastic reduction in the number of nodes for communication. The tree that is formed at the sub-group level is of height $h = 1$ as it is formed of only one level of subordinates reporting to their superior. Moreover the attributes used to identify individual nodes is just the individual identifier (ID). Individual ID is the minimal requirement as access control attribute to represent a member in the sub-group.

Considering a binary ACT tree Table 1 shows that as the number of nodes get reduced by logN factor the size of the public parameters, public key, private key and ciphertext, drastically reduces. The proposed scheme shows evident improvement in efficiency. Here N'_s being just the identifier (ID) of the node takes very few bits hence Private Key K_A is very small. The number of attributes in the ciphertext C also contains only m attributes (considering only ID), which is $m \ll l$, where $l = m^h$ in the case, ACT attributes of the entire tree is considered. This reduces not only the size of the ciphertext but also the complexity of the cryptographic primitives.

Table 1: Comparison of size of Keys and Ciphertext in the proposed Scheme and CP-ABE system

Systems	A	K_M	K_A	C
Waters	$(N^2+2)L_G + L_G 1$	L_G	$(N+N_S+1)L_G$	$(N*l+1)L_G$
ACT-in-HFN	$(\log N+2)L_G + L_G 1$	L_G	$(\log N + N'_S+1)L_G$	$(\log N * m+1)L_G$

As the number of members within an ACT of a group reduces so does the number of attributes in its Universal Attribute set that identifies each member within the group. Therefore, $N_s \gg N'_s$, i.e the size of user's attribute set in Waters is much greater than that of the size of user's attribute set in the proposed system. This is because the number of members in a particular sub-group is far less that the number of members considered in the entire Task Force. For decryption in the original CP-ABE algorithm, threshold access policy had to be evaluated from top of the tree of height h to the leaves to find whether a receiver can decrypt a ciphertext or not. Similar is the case of encryption process also. This requires to traverse the entire tree. But in the proposed scheme only a single level parsing is required as sub-groups form single level trees. This has resulted in enormous reduction in space and time complexity./par Considering ACT as a binary tree, Table 2 shows that the reduction in the total number of nodes have improved computational complexity by a factor of logN. In CP-ABE based access control both encryption and decryption complexity time is O(N), where N gives the size of the universal attributes of the system. The proposed system improves over the conventional CP-ABE based access control by improving over the time complexity of encryption and decryption algorithm, which is $O(\log N)$.

Table 2: Comparison of computational time in Proposed Scheme CP-ABE system

Systems	Key Generation	Encryption	Decryption
Waters	$(N*N_S+1)T_G$	$(N+l+1)T_G + 2T_G 1$	$(N*l)T_G + (N+I+1)T_G 1$
ACT-in-HFN	$(\log N * N'_S+1)T_G$	$(\log N * m+1)T_G + 2T_G 1$	$(\log N * m)T_G + (\log N + I'+1)T_G 1$

The network can be more scalable provided the organizational structure of the Task Force remains the same. The private key can be saved in the node prior to deployment. Increase in the number of nodes can be tolerated to some extend without increasing time complexity and the key size. Reduction in attribute set has been made possible by using a forest of ACTs. Each group executes the CP-ABE algorithm for secure and privacy preserving communication within the sub-group and is independent of other subgroups within the Task Force.

4 Conclusion

The proposed system provides an efficient solution in applications which demands secured and privacy preserving group communication in hastily built networks with limited infrastructure. The proposed algorithm compared to the conventional algorithm exhibits high performance. This is achieved by dividing the Task Force into sub-groups for group communication. Task Force being organized in Line-and -Staff organization structure, group communication is required only between the authority and his subordinates. This results in ACT and the access policy having fewer public parameters to compare. It is very well established that reducing the size of attribute set brings down the complexity of the implementation of CP-ABE in Hastily Formed Networks. The proposed scheme is a generalized solution for any Task Force formation for application that requires restricted access to secret information. It pays less overhead cost for high performance as compared to the conventional methods. Though the proposed scheme would work well for Task Force that are static in its organization, but it would become unsuitable for those applications where the organizational structure, as a whole, changes dynamically. Like, if suppose an entire level in the organizational structure is removed (except for the highest and lowest), then the proposed algorithm is not that effective. The future scope of research in line with the proposed scheme is to refine it such that it can adapt to changing organizational structure of the Task Force.

References

[1] Multimedia Applications for MANETs over Homogeneous and Heterogeneous Mobile Devices. `http://www.apec.org/groups/som-steering-committee-on-economic-and-technical-cooperation/workinggroups/emergency`.

[2] H. Aldabbas, T. Alwada'n, H. Janicke, and A. Al-Bayatti. Data confidentiality in mobile ad hoc networks. *International Journal of Wireless & Mobile Networks*, 4(1):225–236, February 2012.

[3] S. A. Alomari and P. Sumari. *Wireless Communications and Networks - Recent Advances*, chapter 22. Multimedia Applications for MANETs over Homogeneous and Heterogeneous Mobile Devices. InTech, 2012.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *Proc. of the 28th IEEE Symposium on Security and Privacy (SSP'07), Oakland, California, USA*, pages 321–334. IEEE, May 2007.

[5] G. A. Bigley and K. H. Roberts. The incident command system: High-reliability organizing for complex and volatile task environments. *The Academy of Management Journal*, 44(6):1281–1299, December 2001.

[6] D. Boneh. The decision diffie-hellman problem. In *Proc. of the 3rd International Symposium, Algorithmic Number Theory (ANTS'98), Portland, Oregon, USA, LNCS*, volume 1423, pages 48–63. Springer-Verlag, June 1998.

[7] H. Choi, P. McDaniel, and T. F. L. Porta. Privacy preserving communication in manets. In *Proc. of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'07), San Diego, California, USA*, pages 233–242. IEEE, June 2007.

[8] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In *Proc. of the 13th ACM conference on Computer and communications security (CCS'06), Alexandria, Virginia, USA*, pages 99–112. ACM Press, October-November 2006.

[9] A. Sahai and B. Waters. Fuzzy identity-based encryption. In *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark, LNCS*, volume 3494, pages 457–473. Springer-Verlag, May 2005.

[10] A. Shamir. Identity-based cryptosystems and signature schemes. In *Proc. of the Advances in Cryptology (CRYPTO'84), Santa Barbara, California, USA, LNCS*, volume 196, pages 47–53. Springer-Verlag, August 1984.

[11] G. Sun, Y. Dong, and Y. Li. Cp-abe based data access control for cloud storage. *Journal of China Institute of Communications*, 32(7):146–152, July 2011.

[12] B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Proc. of the 14th International Conference on Practice and Theory in Public Key Cryptography (PKC'11), Taormina, Italy, LNCS*, volume 6571, pages 53–70. Springer-Verlag, March 2011.

Author Biography

Biji Nair received the B.E. and M.E. degrees in Computer Science and Engineering from University of Calicut, Kerala, India and Cochin University of Science and Techonology, Kerala, India. Presently pursuing Ph.D in National Institute of Technology, Trichy, Tamil Nadu, India. Her research areas includeWireless Sensor Networks, Lightweight Cryptography and Natural Language Processing.

M. Sridevi is working as an Assistant Professor in National Institute of Technology (NIT) Trichy,India since 2008. She received Ph.D. from NIT, Trichy in 2015. Her research interests include Image Processing, Parallel Algorithms and Optimization Techniques.

C. Mala is currently serving as an Associate Professor in the Department of Computer Science and Engineering, National Institute of Technology, Trichy, India. She received Ph.D. from National Institute of Technology, Trichy in 2008. Her research interests include Wireless Networking, Parallel Algorithms, Soft Computing and Image Processing.

Lakshmi Prabha S is a post doctoral fellow in the department of Computer Applications, National Institute of Technology, Tiruchirappalli (NITT), India. She worked as an Assistant Professor at Srinivasa Ramanujan Centre, SASTRA University, India. She completed her Ph.D., in 2015 in NITT, India. Her research interests include Pure Graph Theory, Graph theory and its applications to Graph algorithms, Social Networks, Group Dynamics, Social Psychology, Business and Management.