Multilevel Access Control in a MANET for a Defense Messaging system using Elliptic Curve Cryptography

J. Nafeesa Begum nafeesa_jeddy@yahoo.com
Sr.Lecturer/CSE
Government College of Engineering,Bargur
Krishnagiri District,Tamil Nadu,India

K.Kumar pkk_kumar@yahoo.com
Lecturer/CSE
Government College of Engineering,Bargur
Krishnagiri District,Tamil Nadu,India

Dr.V.Sumathy sumathy_gct2001@yahoo.co.in
AssistantProfessor/ECE
Government College of Technology,Coimbatorer
Coimbatore District,Tamil Nadu,India

Abstract

The trend of the Civilian society has moved from the industrial age focus on automation and scale towards information based on computing and communication. Today's Warfare is also moving towards an information age paradigm based on information sharing, situational awareness, and distributed points of intelligence, command and control. A widely-networked fighting force is better able to share information about tactical situations that may be geographically widespread, asymmetric, and rapidly changing. Commanders must be able to better assess situations across broad theaters, with extensive data, voice, and especially video feeds as strategic inputs. Thus, network-centric warfare improves effectiveness at both the tactical "point of the spear" and in the achievement of broader strategic goals. Broadly disseminated knowledge assets enable fighting forces that must self-synchronize, even as they physically disperse to address dynamic battlefield conditions. The speed of decision has increased and command decisions must be rapidly relayed and implemented, to improve battlefield outcomes. Multilevel access control in a MANET for a Defense messaging system is used to have the command decisions relayed to all people who are active in the group and also to all people who have been identified as higher in the hierarchy instead of sending one to one messages to each individual.. The system developed is secure, multi site and allows for global communication using the inherent properties of Elliptic Curve cryptography . Elliptic Curve cryptography provides a greater security with less bit size and it is fast when compared to other schemes. The implementation suggests that it is a secure system which occupies fewer bits and can be used for low power devices**.**

Keywords: Defense messaging system,Elliptic Curve cryptography, Encryption , Global Information Sharing , Secure system.

1. INTRODUCTION

Information superiority has become as important in today's battlefield as air superiority was in the past in increasing mission effectiveness. Information superiority has become critical as needs of both war fighters and commanders have broadened to include real-time video, high-speed data, and voice. Data and intelligence sources include terrestrial forces and sensors, satellites, UAVs (Unmanned Aerial Vehicles), and a wide variety of centralized and distributed information assets.[7,8] The vast majority of these information assets, command, communications, and control must be delivered wirelessly, with seamless connections to wired networks for intelligence resources and other data. Further, these wireless technologies must support data, voice, and increasingly, video traffic flows. In the network-centric warfare environment, mobility implies more than just the motion of individuals and vehicles in relation to one another and to other fixed locations.

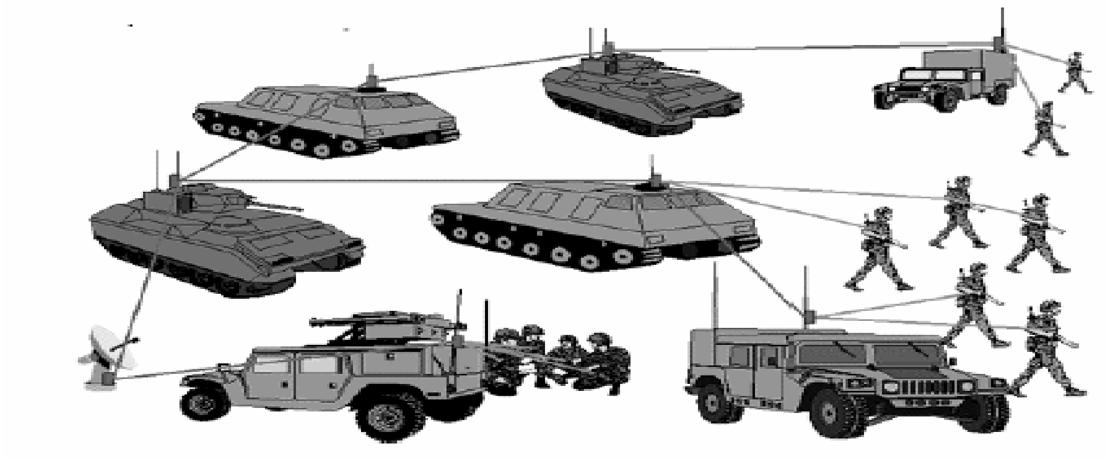


Figure:1 MANET In a military warfare

In such a mobile adhoc network a Defense messaging system takes a message and forwards it to the intending recipients or parties based on the message criteria for immediate action. It enables the top defense personnel to issue commands using messages to guard the country against threats of terrorists, anti socials and Intruders. The system developed has the following capabilities

- Encryption of the data stream
- Strong user authentication
- Prevention of interaction with external and undesirable applications
- Platform independent
- Central administration and logging

As a multilevel access control systems, the system developed has the following features

- Hiding of hierarchy and receivers
- Authentication of receivers
- Dynamics at message level, class level and user level by the server

The main advantage of ECC compared to other schemes is that it offers equal security with a smaller key size and thus reduces processing overhead and can be used in Tiny devices also. The rest of the paper is as follows. Section 2 gives the related work Section 3 describes Elliptic Curve Cryptography. Section 4 explains our system development, algorithms and dynamics. Section 5 gives the implementation results, Section 6 does the Performance Analysis and Section 7 concludes the paper.

2.RELATED WORK

The first multi level access solution was proposed by Akl et al.[1] in 1983 and followed by many others [8,9,10,11,13,14,15,16 ,12]. These schemes basically rely on a one-way function so that a node v can easily compute v's descendants' keys whereas v's key is computationally difficult to compute by v's descendant nodes. Moreover, many existing schemes have some of the following problems: (1) Some schemes were found with security flaws shortly after they were proposed [3,4] (2) Some schemes cannot support for reconfiguration of a hierarchy [18,19]; (3) Some schemes require access hierarchy to be in a certain form so that it must be a tree or a DAG with only one root; and (4) Member revocation is one of the most difficult processes in cryptographic schemes, therefore, it is important to address this problem so that the revocation process can be dealt with efficiently. In this paper, we propose a new scheme based on elliptic curve cryptography for secret messaging which has the suitable characteristics. Unlike many existing schemes based on one-way functions, our scheme is based on a secret sharing method which makes the scheme unconditionally secure [17, 20] .Elliptic curve cryptography address the issue of saving the power due to the use of less number of bits for secure transmission [2]. In our previous work we have used [5,6] Elliptic curves used for efficient group key management. In this paper we have extended it to include multilevel access control. Multilevel access control using elliptic curve cryptography is a new research area under deployment and we have used it in the defense messaging system so that higher group members can see the messages relayed to lower group members.

3. ELLIPTIC CURVE CRYPTOGRAPHY

3.1 Basics

Elliptic curves are named so as they appear to be similar to the equation defining the roots of an ellipse. They are equations containing two variables and coefficients where the elements are in a finite field (Z_p) . The elliptic equation is of the form $y^2 = x^3 + ax + b$. The coefficients a,b should satisfy the condition $4a^3 - 27b^2 \neq 0$ so that there are no repeated factors. For given values of a and b , the elliptic curve consists of positive and negative values of y for each value of x. A special point O which acts as an identity is used. The following addition rules are used in elliptic curve arithmetic.

1. P + O = O +P = P for all P belongs to Zp
2. If P = (x, y) Є E (Zp) then (x, y) +(x, -y) = o and is called the negative of P and –P is a point on the curve.
3. Let P =(x_1,y_1) Є E (Zp) Q =(x_2,y_2) Є E (Zp) where P≠Q then P + Q is =(x_3,y_3)
   $x_3 = (\lambda^2 - x_1 - x_2)$mod P
   $y_3 = (\lambda (x_1 - x_3) - y_1)$ mod P and
   $\lambda = ((y_2 - y_1) / (x_2 - x_1))$ mod P if P ≠ Q
   $\lambda = ((3x_1^2 + a) / 2y_1)$ mod P if P = Q
4. Multiplication is defined by repeated addition

In case of a finite group Ep(a, b) the number of points on the elliptic curve is bounded by $P+1 - 2\sqrt{P} \leq N \leq P + \sqrt{P}$ so that for a large P ,the number of elements is approximately equal to P.

3.2 Algorithm For Elliptic Curve Cryptography

Step1: Decide on the elliptic curve E .The Elliptic curve should have two coefficients a,b such that $4a^3 - 27b^2 \neq 0$ and p a prime number.
Step2: For the elliptic curve equation apply values of x from 1 to p-1 and generate y values.
Step3: Find the Quadratic residues to avoid repetition in mod values.
Step4: Collect all the points on the elliptic curve.

Step5 : Use one point called the base point as the generator using which scalar multiplications are performed and generate multiples of the generator by applying the ECC arithmetic rules.
Step 6: For a same elliptic curve, by choosing a different generator point we can obtain a different encryption values.

3.3. Example

Points in Elliptic Curve :The Points in $E_{211}(0,-4)$ are found using steps 1 to 5.

1,29	1,182	2,2	2,209	5,11	5,200	6,1	6,210	12,6	12,205
13,100	13,111	14,29	14,182	16,100	16,111	17,30	17,181	19,37	19,174
20,20	20,191	21,87	21,124	23,66	23,145	24,59	24,152	26,103	26,108

Table: 1 Some Points in $E_{211}(0,-4)$

Using (2,2) as Generator point ,we get the multiple point scalar multiplication of generator from 0 to Infinite Limit. Let 1 G = (2 , 2) to generate 2 G we perform scalar Multiplications G + G = 2G and using the formulae

$x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda (x_1 - x_3) - y_1$ and $\lambda = (y_2 - y_1) / (x_2 - x_1)$ if $P \neq Q$
$\lambda = 3x_1^2 + a / 2y_1$ if $P = Q$
$= 12/4 = 3,$
$x_3 = 9 - 2 - 2 = 5,$
$y_3 = 3(2-5) - 2 = 3(-3) - 2 = -11 \bmod 211 = 200$

ANS:5,200

3.4.Generation of Points using Scalar Multiplication

To get 3G we add G (2,2) to 2 G (5,200) we get different P values as shown below

2,2	5,200	129,56	159,114	153,108	125,152	179,199	174,163	111,145	75,90
168,6	155,96	21,87	201,85	28,2	181,209	150,85	198,139	161,142	54,138
27,30	84,210	87,50	192,201	69,20	51,136	182,100	64,194	29,139	70,200

Table:2 The Scalar Multiplication points for $E_{211}(0,-4)$ at G(2,2)

This procedure is used for generating different elliptic curves. In fact we can use the same elliptic curve for all classes by changing the generator value. For the above points we can generate 240 different sets each containing 240 points for encryption.

4.Elliptic Curve Cryptography for defense messaging system

4.1.System Overview

Multilevel Access Control in Manet for a defense messaging system is useful for military organizations which have a hierarchical structure. For example in the Indian Military System the following hierarchy exists.

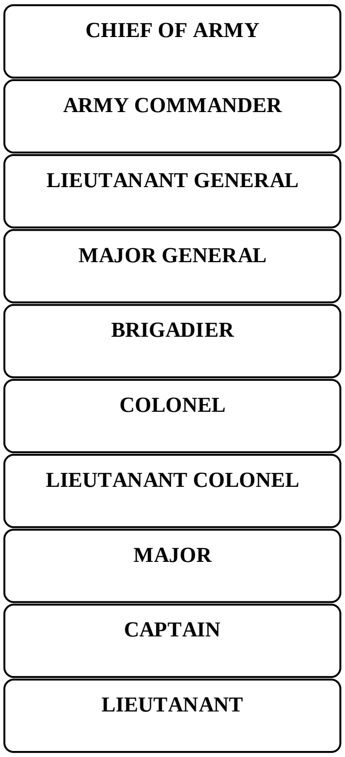


Figure 2 : Military hierarchy

In such a type of system, messages sent to a lower class should be known to the active members of lower class and also to all active members of the higher class. It is not only essential to maintain the access control but the data should be hidden as well. Elliptic curve cryptography technique is used .

There are many messages to be sent to different parties. The server inserts new data streams according to the classification . The messages are encrypted using ECC according to the access allowed for each user and ,the data is sent . Consider the following set of messages.

Class	Category of Data Streams			
	Confidential	Field Messages	Terror Messages	Climate Warning
Troops	×	√	×	×
Air Wing	×	×	×	√
NSGS	×	×	√	×
Lieutenants	√	√	×	×

Table:3 Example Showing Message classifications

All the users of defense messaging system need to register themselves and get authenticated by the server. Once the registration process is over the user when joins receives the message he is entitled to receive .Only authenticated users are able to view the message content as the message remains unintelligible to people who do not belong to that elliptic curve. Different Elliptic curves identify different class of users .the servers contribution and the users contribution are used for finding the Group keys.

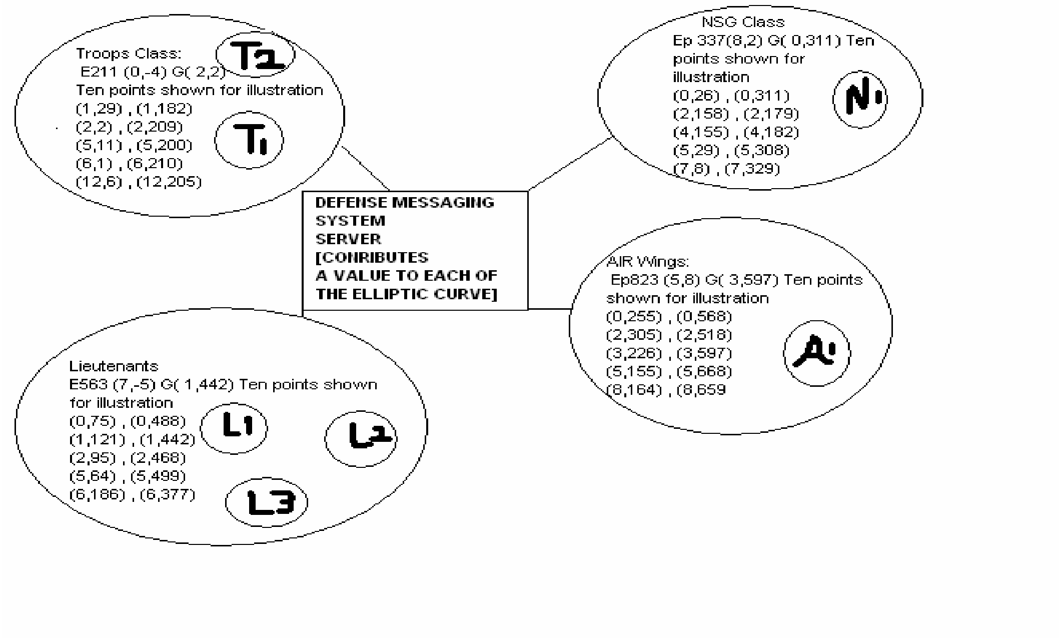


Figure 3 :System Overview

L1,L2,L3 belongs to lieutenant group ..N1 is National Security Guard ,T1,T2 are troops and A1 is a Air wing Officer.

4.2 The Proposed Scheme

The following methodology is used for developing a multilevel access control solution in a Manet for a defense messaging system using Elliptic Curve Cryptography.

Step1: The server or the central authority creates different classes with different service requirements. The system is dynamic and any hierarchy can be created or modified. The classes are arranged as a Tree based structure. A class can have any number of descendent classes at the next level and a class can have any number of users .
Step2 : Each class maintains a list of its ancestor and descendent classes.
Step 3: Each class is associated with an elliptic curve E : y2 = (x3 + ax+ b) mod p over Zp and G = E(Zp)is a Generating point.
Step 4: Users generate a random number as their contribution value and join their classes. The Shared secret key for each class is calculated whenever user joins or leaves .
Step 5: One user in each class is designated as the class controller . The user joining last is usually given the role of the class controller .
Step 6: The class controller of each class initiates the process of changing the group key Whenever users join or leave . Hence forward secrecy and backward secrecy is strictly maintained and only active members of the particular class will be able to view the message transfer of that particular class.
Step 7: Whenever the class controller leaves , the user who joined the class before the class controller now becomes the class controller. This is based on the assumption that a person who joins late will leave late which is many times true. The group key is changed in this case also so that the old class controller should not be able to decrypt the message.
Step 8: The group key is sent to all the ancestor class controller nodes by the class controller.
Step 9: The messages are also sent to the ancestor class controllers.

Step10. The messages received by the ancestor class controller will be decrypted by sender's group key and again encrypted with their own group key and sent to all users of that class .The users will use only their Group key to decrypt ,so users need to remember only their group key . A user who is also a class controller should remember his group key and also the group key of all its descendent classes.
Step 11: This system is efficient because all dynamics of a class are local to that class only and only one message is sent to the ancestor class controllers .
Step 12: All users of a higher level class are not disturbed by the dynamics of the lower class and also they receive the messages from their class controller.
Step 13: The Central Authority is less burdened as all the message transfers are local among the class controller.

4.3 System Dynamics

1. Message stream Dynamics: New data streams are encrypted and send by the server. There is a facility to add new items as and when the need arises for the defense messaging system.
2. Class Dynamics: New Classes can be added by using a new curve and what messages should be included for the new classes can be set
3. User Dynamics: User may join or leave .Whenever a user joins, he is authenticated and group key is calculated. Whenever the user leaves the group key of that particular class gets changed .Hence forward secrecy and backward secrecy are maintained.

4.3 ECC Key Exchange Mechanism :

The key exchange is an analogue of the Diffie Hellmann scheme. The server uses a different random number as the contribution for each of the curves. The Elliptic curves are decided before hand and each class user comes in a separate elliptic Curve. The Group keys are used for getting the messages encrypted. It is found to be very secure.
Users joining the Troop class is shown below

The Server Joins

User Id: Server Private Key (nA) = 47568
Public key (A) = g^{nA} = (nA mod p) G = (47568 mod 241) G

= 91 G = (206,121)

Troop User1 Joins

User Id: TUser1 Private Key (nB) = 13525
Public key (B) = g^{nB} = (nB mod p) G = (13525 mod 241) G

= 29 G = (29,139)

<u>Finding the Group key after One Troop user and Server joined the group</u>

Server Calculates the Group key
Server will get g^{nB} from $TUser_1$ i.e. (29,139) yields 29
Shared key = g^{nAnB}
= ((47568*29)mod 241) G
= 229 G
= (155,115)
Troop User1 Calculates the Group key
$TUser_1$ will get g^{nA} from Server i.e. (206,121) yields 91
Shared key = g^{nAnB}

= ((13525*91)mod 241) G
= 229 G
= (155,115)

Troop User$_2$ Joins the Group

User Id: TUser2 Private Key (nC) = 82910
Public key (C) = g^{nC} = (nC mod p) G = (82910 mod 241) G
= 6 G = (125,152)

Finding the Group key after the Second Troop User joined the Group

The new TUser2 act as a Group controller.
TUser2 computes g^{nBnC} , g^{nAnC}
g^{nA} = (206,121) yields 91
g^{nAnC} = (91*82910 mod 241) G = 64 G = (147,97)
g^{nB} = (29,139) yields 29
g^{nBnC} = (29*82910 mod 241) G = 174 G = (131,84)
Sends the g^{nBnC} Value to Server and g^{nAnC} Value to TUser1.

Finding the Group key after three users joined the group

Server Calculates the Group key

server will get g^{nBnC} from TUser$_2$ (GC) i.e. (131,84) yields 174
Shared key = g^{nAnBnC}
= ((47568*174)mod 241) G
= 169 G
= (120,31)

TUser1 Calculates the Group key

TUser$_1$ will get g^{nAnC} from TUser$_2$ (GC) i.e. (147,97) yields 64
Shared key = g^{nAnBnC}
= ((13525*64)mod 241) G
= 169 G
= (120,31)

TUser2 Calculates the Group key

g^{nAnB} i.e. (155,115) yields 229
Shared key = g^{nAnBnC}
= ((82910*229)mod 241) G
= 169 G
= (120,31)

User Leave from the Group

Let the TUser2 be leave. Then the user sends message to all users that it is leaving. All the users remove the leaving user from the user list. The group controller changes its key value and computes the new group key.
Group controller New Private Key = 43297.
The group controller recalculates the following values:
g^{nAnB}= (155,115) yields 229
Sends the g^{nB} Value to Server, g^{nA} Value to TUser1.
Using the shares the Group keys are calculated

Message Encryption

Message: Enter nestFire
Random Number K_A : **202**
Cipher Text Pc =(K_AG, PM+K_AS_K)

K_AG = 202 G
= 202 mod 241 G
= (50,57)
Cipher text: 50:57:

1:182:164:197:203:180:1:182:172:50:136:11:164:197:
1:182:160:8:203:180:114:113:185:199:172:50:1:182:

$PM+K_AS_K$
PM
e→101 (1,182)
n→110 (164,197)
t→116 (203,180)
e→101 (1,182)
r→114 (172,50)
(Space)→32 (136,11)
n→110 (164,197)
e→101 (1,182)
s→115 (160,8)
t→116 (203,180)
f→102 (114,113)
i→105 (185,199)
r→114 (172,50)
e→101 (1,182)
K_AS_K = (202 * 18) mod 241
= 21
$PM+K_AS_K$
e= (101+21) mod 241
= 122 G
= (156,10)
n=(110+21) mod 241
=131 G
=(164,14)
t = (116+21) mod 241
= 137 G
= (163,161)
e= (101+21) mod 241
= 122 G
= (156,10)
r = (114+21) mod 241
= 135 G
= (77,145)
= (32+21) mod 241 (for space)
= 53 G
= (99,180)
n =(110+21) mod 241
=131 G
=(164,14)
e = (101+21) mod 241
= 122 G
= (156,10)
s = (115+21) mod 241
= 136 G
= (185,12)
t = (116+21) mod 241
= 137 G = (163,161)

f = (102+21) mod 241
= 123 G
= (104,190)
i = (105+21) mod 241
= 126 G
= (160,203)
r = (114+21) mod 241
= 135 G
= (77,145)
e = (101+21) mod 241
= 122 G
= (156,10)

Message Decryption

The Group Key (S_k) is (198,139)
Random no. Chosen can be found by the K_AG Value (50,57).

From (50,57) we may trace the value K_A as 202.

(1)PM+K_AS_K = (156,10)

PM = (156,10) - K_AS_K
= (156,10) -21
= 122 – 21
= 101 G => (1,182) → e

(2) PM+K_AS_K = (164,14)

PM = (164,14) - KASK
= (164,14) -21
= 131 – 21
= 110 G => (164,197) → n

(3) PM+K_AS_K = (163,161)

PM = (163,161)- K_AS_K
= (163,161) -21
= 137 – 21
= 116G => (203,180) → t

(4) PM+K_AS_K = (156,10)

PM = (156,10) - K_AS_K
= (156,10) -21
= 122 – 21
= 101 G => (1,182) → e

(5) PM+K_AS_K = (77,145)

PM = (77,145) - KASK
= (77,145) -21

= 135 – 21
= 114 G => (172,50) → r

(6) PM+K_AS_K = (99,180)
PM = (99,180) - K_AS_K
= (99,180) -21
= 53 – 21
= 32 G => (136,11) ➔ (Space)

(7) PM+K_AS_K = (164,14)
PM = (164,14) - KASK
= (164,14) -21
= 131 – 21
= 110 G => (164,197) ➔ n

(8) PM+K_AS_K = (156,10)
PM = (156,10) - K_AS_K
= (156,10) -21
= 122 – 21
= 101 G => (1,182) ➔ e

(9) PM+K_AS_K = (185,12)
PM = (185,12) - K_AS_K
= (185,12) -21
= 136 – 21
= 115 G ➔(160,8) ➔ s

(10) PM+K_AS_K = (163,161)
PM = (163,161)- K_AS_K
= (163,161) -21
= 137 – 21
= 116G => (203,180) ➔ t

(11) PM+K_AS_K = (104,190)
PM = (104,190) - K_AS_K
= (104,190) -21
= 123 – 21
= 102 G => (114,113) ➔ f

(12) PM+K_AS_K = (160,203)
PM = (160,203) - K_AS_K
= (160,203) -21
= 126– 21
= 105 G => (185,199) ➔ i

(13) PM+K_AS_K = (77,145)

PM = (77,145) - KASK
= (77,145) -21
= 135 – 21
= 114 G => (172,50) ➔ r

(14) PM+K_AS_K = (156,10)
PM = (156,10) - K_AS_K
= (156,10) -21
= 122 – 21
= 101 G => (1,182) ➔ e

4.4.Elliptic Curves used

Troops Class:

$y^2 = x^3 - 4 \mod 211$ at G(2,2)

NSG Class: (National Security Guards)

$y^2 = x^3 + 8x - 2 \mod 337$ at G(0,311)

Lieutenants:

$$y^2 = x^3 + 7x + 5 \mod 563 \text{ at } G(1,442)$$

AIR Wings:

$$y^2 = x^3 + 5x - 8 \mod 823 \text{ at } G(3,597)$$

4.5.Example Message:

```
Sent....3:Leutanats:TerroristInformation:440:400:487:137:493:111:355:172:325:238:54:289:325:2
38:493:111:215:360:16:73:505:466:505:466:538:236:505:466:293:20:560:148:478:249:378:490:1
51:196:408:337:538:236:505:466:552:448:558:532:478:249:293:20:538:236:151:196:493:111:91:
401:325:325:325:325:493:111:91:401:154:529:493:111:347:141:347:141:2:468:493:111:91:401:3
47:141:154:529:493:111:487:137:347:141:347:141:493:111:487:137:110:102:493:111:151:196:3
4:407:84:311:84:311:493:111:151:196:34:407:84:311:84:311:493:111:151:196:34:407:84:311:84:
311:493:111:151:196:34:407:84:311:84:311:493:111:347:141:325:325:341:438:493:111:487:137:
487:137:154:529:493:111:151:196:34:407:84:311:84:311:493:111:151:196:34:407:84:311:84:311
:493:111:347:141:2:468:329:421:493:111:91:401:347:141:154:529:493:111:154:529:493:111:487
:137:91:401:91:401:493:111:215:203:493:111:91:401:154:529:110:102:493:111:341:438:325:325
:493:111:347:141:347:141:341:438:493:111:487:137:325:325:493:111:347:141:110:102:110:102:
493:111:347:141:2:468:329:421:493:111:91:401:347:141:154:529:493:111:347:141:110:102:215:
203:493:111:487:137:487:137:91:401:493:111:347:141:2:468:329:421:493:111:91:401:347:141:1
54:529:493:111:347:141:341:438:487:137:493:111:347:141:347:141:325:325:493:111:91:401:32
5:325:2:468:493:111:347:141:110:102:347:141:493:111:341:438:325:325:493:111:347:141:347:1
41:341:438:493:111:347:141:329:421:325:325:493:111:487:137:347:141:329:421:493:111:215:2
03:493:111:91:401:154:529:110:102:493:111:341:438:325:325:493:111:347:141:347:141:341:43
8:493:111:91:401:325:325:325:325:493:111:487:137:347:141:341:438:493:111:347:141:110:102:
347:141:493:111:91:401:110:102:91:401:493:111:347:141:110:102:215:203:493:111:487:137:48
7:137:91:401:493:111:341:438:325:325:493:111:347:141:347:141:341:438:493:111:91:401:215:2
03:91:401:493:111:91:401:154:529:341:438:493:111:347:141:329:421:325:325:493:111:487:137:
347:141:329:421:493:111:91:401:341:438:341:438:493:111:347:141:347:141:341:438:493:111:3
47:141:329:421:325:325:493:111:487:137:347:141:329:421:493:111:347:141:329:421:325:325:4
93:111:487:137:347:141:329:421:493:111:151:196:34:407:84:311:84:311:493:111:151:196:34:40
7:84:311:84:311
```

5 IMPLEMENTATION RESULTS:

The system was developed in Java net beans and run on a network. Some sample output screens are shown

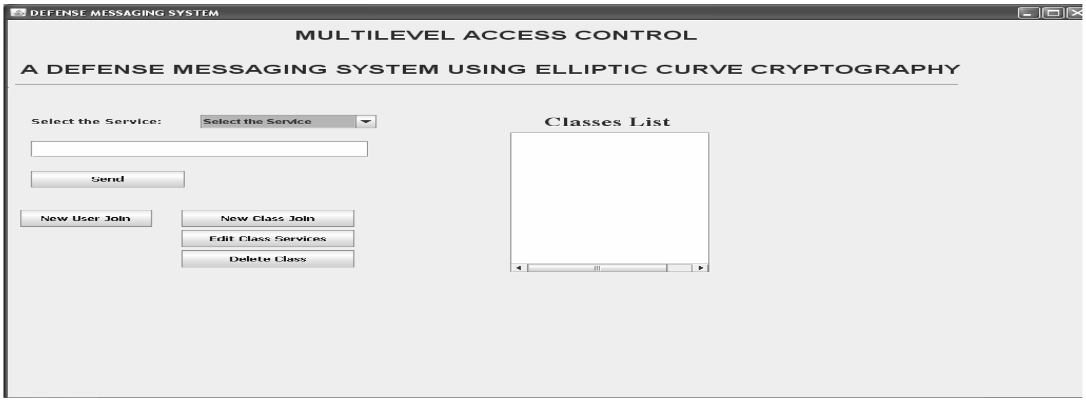


Figure:4 Main Page

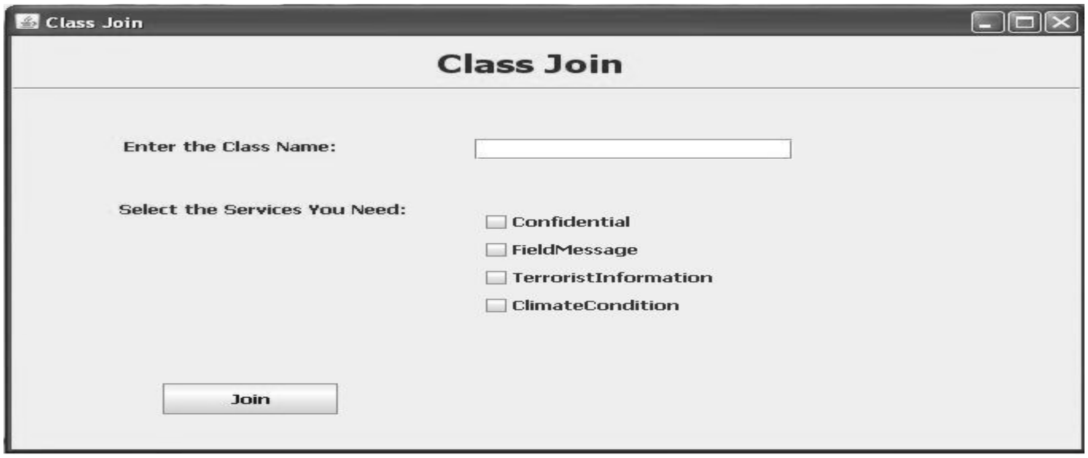


Figure:5 Class Join

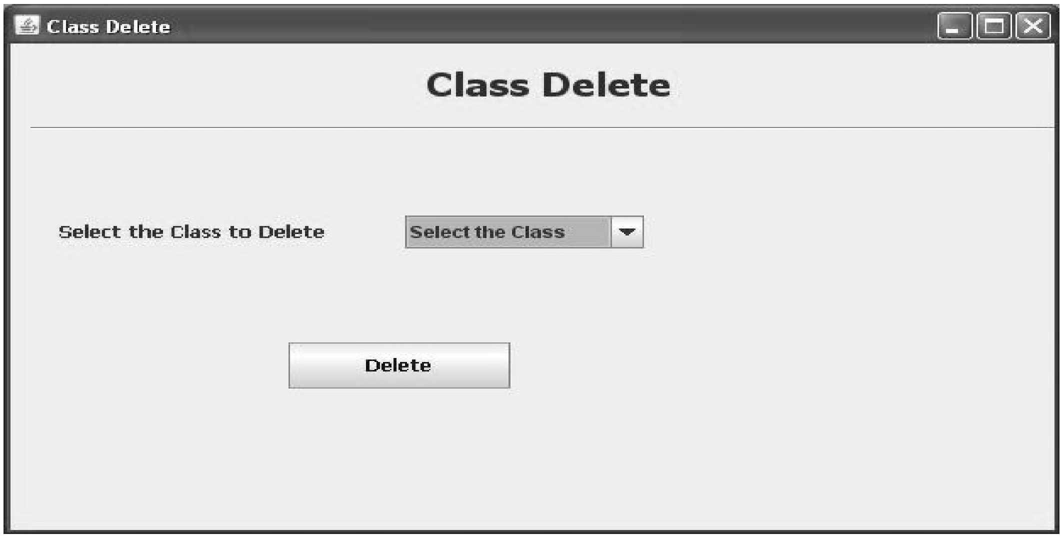


Figure:6 Class Delete

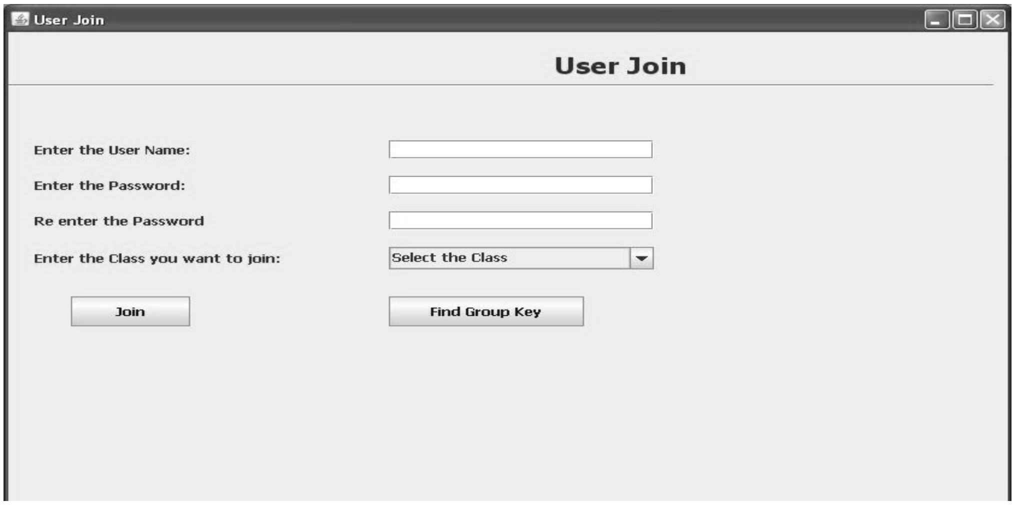
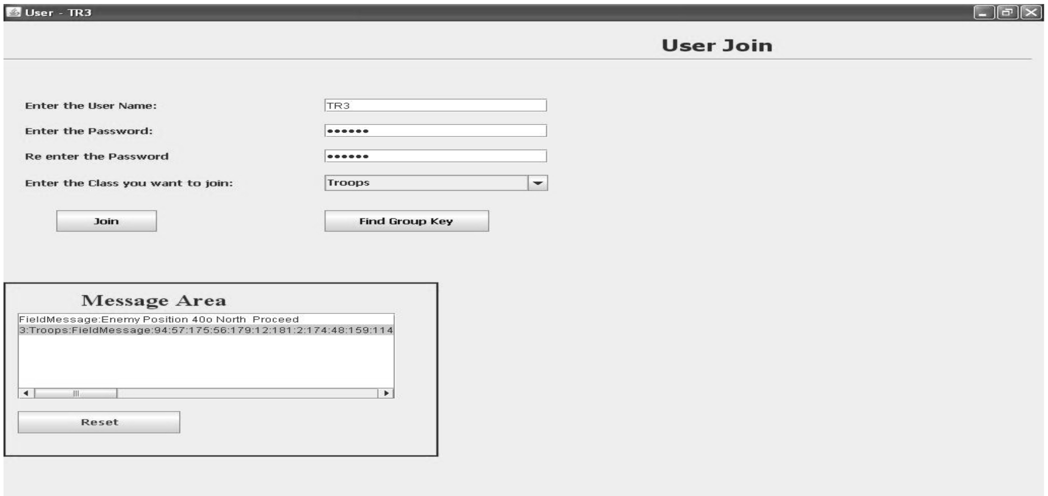


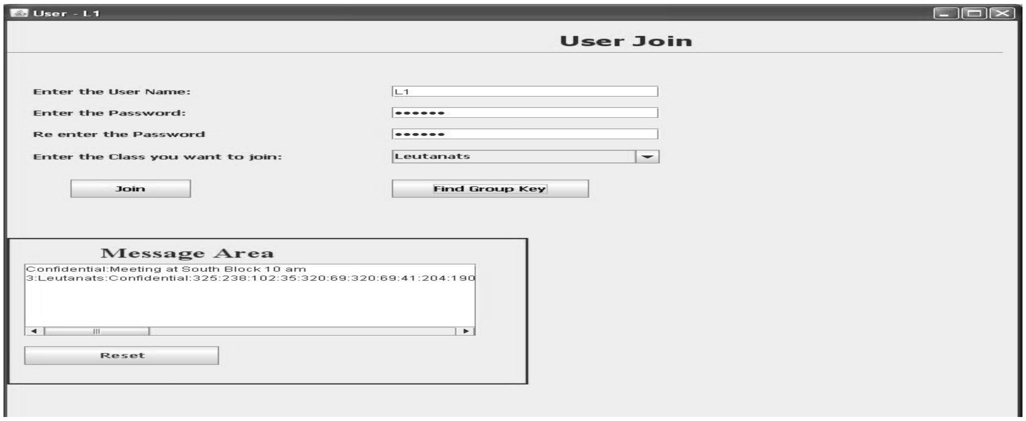
Figure:7 User Join



Enter the User Name: TR3
Enter the Password: ••••••
Re enter the Password ••••••
Enter the Class you want to join: Troops

```
FieldMessage:Enemy Position 40o North  Proceed
3:Troops:FieldMessage:94:57:175:56:179:12:181:2:174:48:159:114
```

Figure :8 Message Received Encrypted and decrypted



Enter the User Name: L1
Enter the Password: ••••••
Re enter the Password ••••••
Enter the Class you want to join: Leutanats

```
Confidential:Meeting at South Block 10 am
3:Leutanats:Confidential:325:238:102:35:320:69:320:69:41:204:190
```

Figure :9 Message Received Encrypted   And Decrypted by lieutenant class

6. PERFORMANCE ANALYSIS:

6.1. Security :

The Security of ECC is due to the discrete logarithm problem over the points on the elliptic curve. Cryptanalysis involves determining x given Q and P where P is a point on the elliptic curve and Q = x P that is P added to itself x times. The best known algorithm to break the elliptic curve points is the pollard – rho algorithm which is a fully exponential algorithm and difficult o solve.. Forward and Backward secrecy are maintained as each session is considered as a separate session. In this section we discuss some attacks and prove that our scheme is secure and feasible. Consider the Figure 10

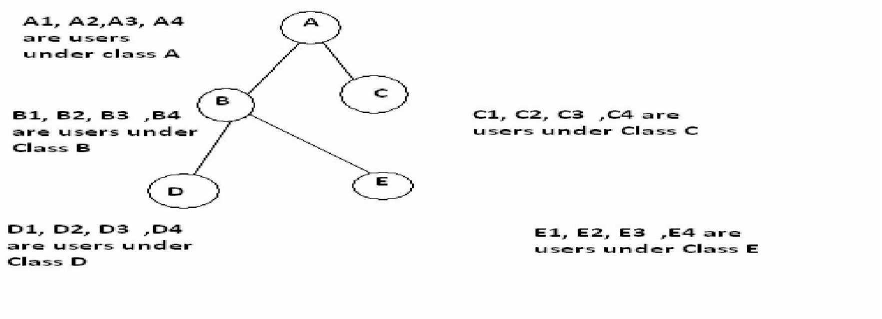


Figure :10 Illustration for security

Attack 1: Contrary Attacks
Assuming that E1 (lower privileged user) wants to crack the secret key of B1 (Higher Privileged User). It is not possible to decrypt any messages as the hierarchy does not provide secret keys to descendent classes. Without knowing the secret key it is impossible to see the message.

Attack 2: Interior Collecting Attacks
If a lower level User has many ancestors and if it negotiates with one parent also by knowing the key as there is no relation parameter between any of the ancestor nodes it is not possible to derive the key.

Attack 3: Exterior Collecting Attack
If an attacker is outside the system, it means no idea about what elliptic curve or generator point is being used is known and hence more difficult to attack.

Attack 4: Collaborative Attacks
We assume that if there is a higher privileged user belonging to class B as in figure 10 and there are two descendant classes D and E. Users of D and E cannot perform a collaborative attack as the secret key of any class is calculated only from the contribution of the respective users of the class. If they compromise one user belonging to the higher privileged group to know the key also, there is no communication possible as the class controllers who control the keying process also change dynamically .

Attack 5: Sibling Attacks
Classes who have same parent also cannot crack the key of a sibling class due to the absence of any related parameters among them.

To maintain the secure structure the following things are necessary.
1. The immediate parents should be loyal and the descendant list should be updated.
2. The Class Controller of a Leaving /Changing Class from the tree hierarchy should update their ancestor list.
3. Recalculation of shared secret key by the leaving /changing class should be done by selecting a random value for finding a new group key.

The third point is very Important and the execution of this prevents disloyal ancestors also from finding the key of a left descendant class even if it no longer comes under their control. The most important feature is that only the key is being transferred and only the authorized entities have idea about which elliptic curve is used or generator points that are used. This is a very big advantage as even though an adversary comes across the key pair he may not know the elliptic curve and the generator. Even users inside the system may decrypt the information but they may not be aware about the mechanism that takes place.

6.1.1 Enhanced Security Framework:
The keys are always transmitted as plain text but we have justified that even with the key any attacker will not be able to first of all receive the messages and even if they somehow receive the message and the key , they will not be able to decrypt the information as they are unaware about the elliptic curve. If security needs to be enhanced the following framework can be included

1. All first level ancestor – descendant pairs use Diffie- Hell man key exchange and generate a key which can be used for encrypting and decrypting the actual key.
2. This key can again be combined with other descendant classes. For e.g., in our sample hierarchy first we perform key exchanges and get the shared secret keys SSK BA, SSK CA and then again use classes D and E and generate SSK DBA ,SSK EBA we can use the resultant keys for encrypting and decrypting the original keys.
4. The above scheme prevents repeated computations

6.2. Memory Cost:

Using ECC approach consumes very less memory when compared to RSA and DES. ECC based approach takes very less memory even the members get increased.

6.3.Communication Costs:

Using other schemes consumes more bandwidth. The Communication and computation of tree based ECDH depends on trees height, balance of key tree, location of joining tree, and leaving nodes. But our approach depends on the number of member in the subgroup, number of Group Controller, and height of tree. So the amount spend on communication is very much less when compared to CRTDH and RSA based scheme.

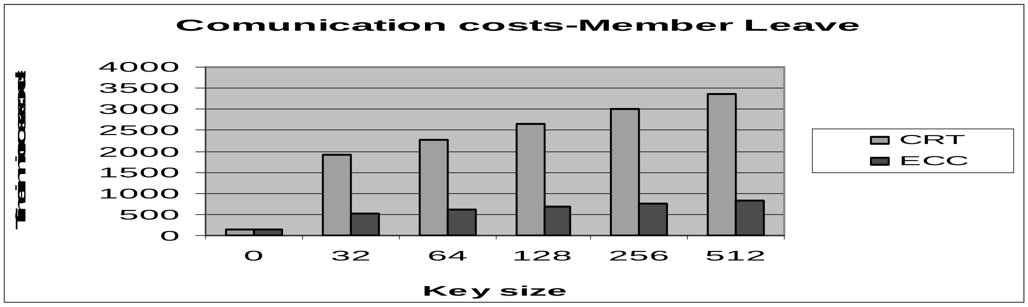


Figure 11.Communication Cost For Member Leave

Consider (Figure.10& 11) there were 256 members in a group our approach consumes only 29% of Bandwidth when compare to CRTDH and RSADH. So our approach consumes low Bandwidth.

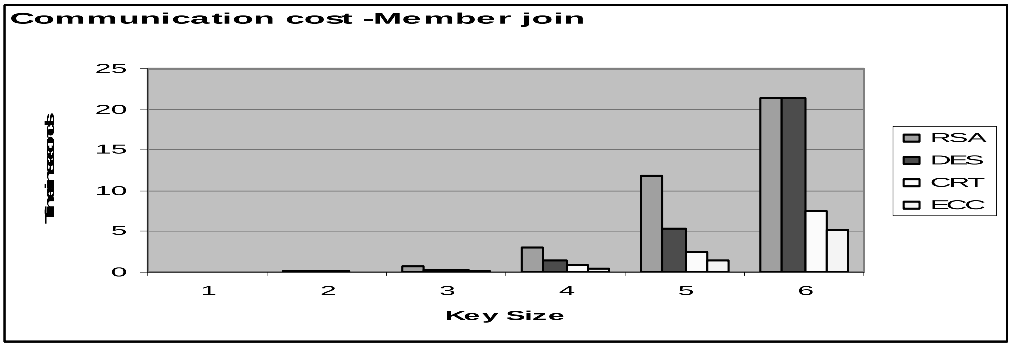


Figure 12. Communication cost for Member Join

For member leave operation also our approach takes less time as the key size for ecc is small compared to other approaches.

6.4. Computation Costs:

The Computational costs depend on the Number of exponentiations. CRTDH have high computation costs as it depends on the number of members and group size respectively. The cost increases as the members and group size increases. But our approach spends a little on this computation. The number of bits for encryption is very less compared to other keys .Moreover each user need not store any data key values.

7. CONCLUSION AND FUTURE WORK:

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons :

Open Medium - Eavesdropping is more easier than in wired network.

Dynamically Changing Network Topology - Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.

Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.

Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.

Lack of Clear Line of Defense – There is a lack of clear line of defense - attack prevention may not suffice.

We have implemented on Multilevel Access Control in a Manet for Defense Messaging System using Elliptic curve cryptography. Use of Elliptic curve ensures that data is protected and intruders cannot guess the message. Moreover a single message sent will reach all the classes which are higher in the hierarchy. The system satisfies the user dynamics and class dynamic. We have successfully implemented by selecting different elliptic curves. A single elliptic curve can be used and by changing the generator points and we can perform different encryption. The group keys are found by the server and forward and backward secrecy is maintained here. The user level, DataStream level and class level hierarchies are taken care. As future implementation new methods for improving parameters can be done..

8.REFERENCES

[1] S. Akl and P. Taylor. “Cryptographic solution to a problem of access control in a hierarchy”. ACM Transactions on Computer Systems, 1(3):239{248,September 1983.

[2] William stallings,” Cryptography and network security Principles and Practices”,Third Edition, Pearson education.2001

[3] M. Atallah, K. Frikken, and M. Blanton,” Dynamic And Efficient Key Management For Access Hierarchies”, CERIAS Tech Report 2006-02,Center for Education and Research in,Information Assurance and Security,Purdue University,

[4] Jason Crampton,”Cryptographically-Enforced Hierarchical Access Control with Multiple Keys”, Journal of Logic and Algebraic Programming April 1, 2009.

[5] K. Kumar J.Nafeesa Begum, Dr.V.Sumathy, (2009), “A Novel Approach towards cost Effective Region Based Group Key Agreement Protocol for Ad Hoc Networks” Computational Intelligence, Communication Systems and Networks ,2009 CICSYN,09 ,July 23-25 2009 published in IEEE Explore.

[6] K.Kumar, J.Nafeesa Begum ,Dr.V.Sumathy , ,,(2009), “ Efficient Region-Based Group Key Agreement Protocols for Ad Hoc Networks using Elliptic Curve Cryptography”,IEEE International Advance Computing Conference(IACC-2009), Thapar University, Patiala March 6-7 . published in IEEE Explore.

[7] Tim Bauge, White paper on "Ad hoc networking in military scenarios", Thales Research and Technology (UK) Limited , May 2004

[8] S. J. MacKinnon, P. D. Taylor, H. Meijer, and S. G. Akl." An optimal algorithm for assigning cryptographic keys to control access in a hierarchy". *IEEE Transactions on Computers*, 34(9):797.802, Sept. 1985.

[9]S. Chen, Y.-F. Chung, and C.-S. Tian. "A novel key management scheme for dynamic access control in a user hierarchy", In *COMPSAC*, pages 396.397, Sept. 2004.

[10] I. Ray, I. Ray, and N. Narasimhamurthi. A cryptographic solution to implement access control in a hierarchy and more. In *SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies*, pages 65.73. ACM Press, 2002.

[11] R. S. Sandhu. "Cryptographic implementation of a tree hierarchy for access control". *Information Processing Letter*, 27(2):95.98, Feb. 1988.

[12] G. C. Chick and S. E. Tavares."Flexible access control with master keys", *Proceedings on Advances in Cryptology: CRYPTO '89, LNCS*, 435:316.322, 1989.

[13] M. L. Das, A. Saxena, V. P. Gulati, and D. B. Phatak." Hierarchical key management scheme using polynomial interpolation". *SIGOPS Operating Systems Review*, 39(1):40.47, Jan. 2005.

[14] L. Harn and H. Y. Lin." A cryptographic key generation scheme for multilevel data security". *Computers and Security*, 9(6):539.546, Oct. 1990.

[15] V. R. L. Shen and T.-S. Chen. ,"A novel key management scheme based on discrete logarithms and polynomial interpolations". *Computers and Security*, 21(2):164.171, Mar. 2002.

[16] M.-S. Hwang, C.-H. Liu, and J.-W. Lo,". An efficient key assignment for access control in large partially ordered hierarchy". *Journal of Systems and Software*, Feb. 2004.

[17] C. H. Lin. "Dynamic key management scheme for access control in a hierarchy. *Computer Communications*,20(15):1381.1385, Dec. 1997.

[18] S. Zhong. A practical key management scheme for access control in a user hierarchy". *Computers and Security*, 21(8):750.759, Nov. 2002.

[19] X. Zou, B. Ramamurthy, and S. Magliveras. "Chinese remainder theorem based hierarchical access controlfor secure group communications". *Lecture Notes in Computer Science (LNCS)*, 2229:381.385, Nov. 2001.

[20] X. Zou, B. Ramamurthy, and S. S. Magliveras, editors." *Secure Group Communications over Data Networks*",Springer, New York, NY, USA, ISBN: 0-387-22970-1, Oct. 2004.