National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

An approach to Elliptical Curve Cryptography to implement Multilevel Access Control in Defence

M. Aishwarya[1], Navya R[2], Pooja D[3], Poojashree K[4]
1Department of Information Science and Engineering, GSSSIETW, Mysuru, Karnataka, India
2Department of Information Science and Engineering, GSSSIETW, Mysuru, Karnataka, India
3Department of Information Science and Engineering, GSSSIETW, Mysuru, Karnataka, India
4Department of Information Science and Engineering, GSSSIETW, Mysuru, Karnataka, India

ABSTRACT

Currently, mobile phones are not only used for formal communication but, also for sending and receiving sensitive information. Sending a message is easy, quick and inexpensive. However, protecting the messages from known attacks like man-in-the-middle attack, reply attack and non-repudiation attack is very difficult. Government and Military Organization have also started using messaging for quick and fast actions. The defence messaging system takes a message and forwards it to the intended recipients or parties based on the message criteria for critical action. This system should provide security assistance and should be manageable by Central Administration Authority. The primary goal of this research is to develop a Multilevel Access Control for Defence Messaging System using Elliptical Curve Cryptography. The system developed is secure, multisite and allows for Global communication using the inherent properties of Elliptical Curve Cryptography It 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, Global communication, Secure system.

I. INTRODUCTION

In a multilevel access control system, users have access to multiple data streams. Defence messaging System is developed to enable the top defence personnel to issue commands using messages to guard the country against threats of terrorists, anti-socials and Intruders. To protect the content from dissemination to unauthorized entities the data streams are encrypted and separate keys are maintained for the purpose. As a multilevel access control system, the system developed has the following features: 1.Communication happens among members of a class 2.Communications taking place among lower classes will be relayed to higher class users 3.Server sends messages to classes when required 4.Authentication of receivers 5.Dynamics at message level, class level and user level. The best schemes for providing multilevel access control is to allow the ancestor nodes to derive the keys of the descendent nodes by some manipulations. Our scheme uses Elliptic curve cryptography to enable secure and efficient multilevel access control. The scheme also supports full dynamics at both user level and class level and permits any random access hierarchies. 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 The rest of the paper is as follows.

II. METHODS AND MATERIAL

A. Overview of ECC Multi level Access Control Protocol:

The goal of this paper is to propose a communication and computation efficient key establishment protocol for defence messaging system. For example, in the Indian Military System the following hierarchy exists. 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.

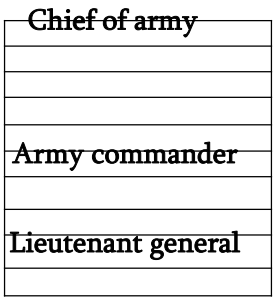

Figure 1. Military hierarchy

It is not only essential to maintain the access control but the data should be hidden as well. 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 message.

Table 1. Example Showing Message classifications

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

All the users of defence messaging system need to register themselves and get authenticated by the server. Only authenticated users are able to view the message content as the message remains unintelligible to people who don't belong to that elliptic curve. Different Elliptic curves identify different class of users.

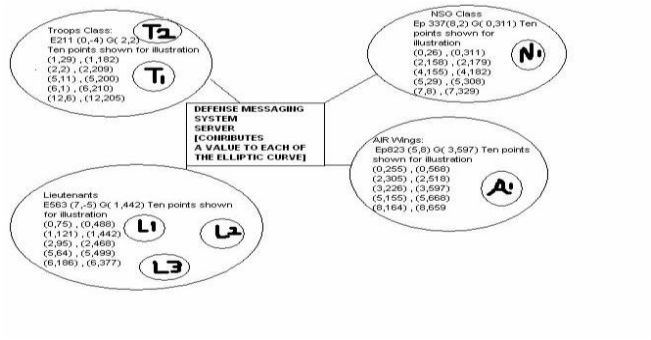

Figure 2. System Overview

B. The Proposed Scheme

The idea is to divide the user classes into several classes according to their hierarchy, let each class have its own subclass key shared by all members of the subclass. Each subclass has subclass controller node and a Gateway node, in which Subclass controller node is the controller of subclass and a Gateway node is controller of subclass controllers.

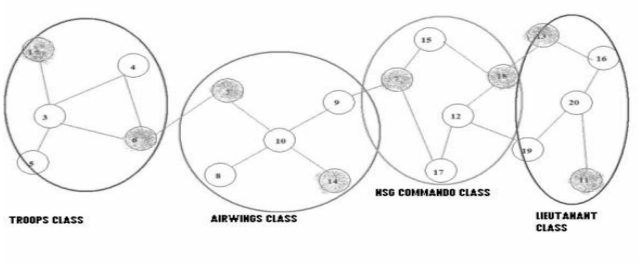

Figure 3. Members of class are divided into subclasses

For example, in Figure.3, all member nodes are divided into number of subclasses and all subclasses are linked in a tree structure as shown in Figure.4

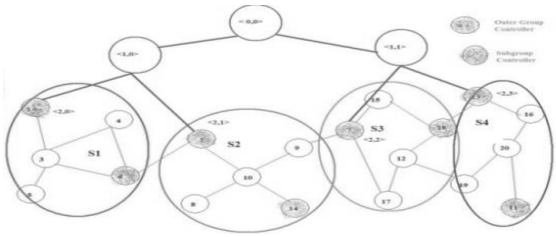

Figure 4. Subclasses link in a Tree Structure

The layout of the network is as shown in below Figure.5.

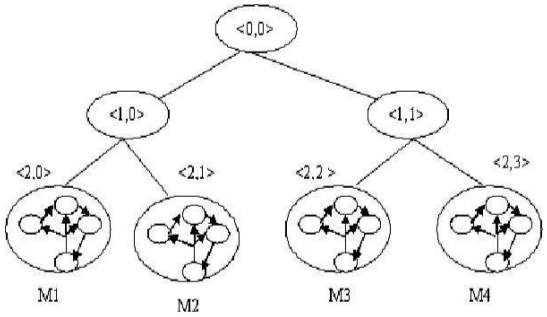

Figure 5. Arrangement of classes

C. Algorithms and Design of ECC Multi level Access Control Protocol:

Assume that there are totally N members in the group Class Communication. After sub classing process (Algorithm 1), there are S subclasses M_1, M_2… M_s with n_1, n_2, n_s members.

Algorithm 1. Multilevel Access Key Agreement

1. The Subclass Formation: The number of members in each subclass is **N / S < 100.**Where, N – is the class size and S is the number of subclasses. Assuming that each subclass has the same number of members.

2.The Contributory Key Agreement protocol is implemented among the class members. It consists of three stages.

a. To find the Subgroup Controller for each subgroups

b. ECGDH protocol is used to generate one common key for each subgroup headed by the subgroup controller.

c. Each subgroup gateway member contributes partial keys to generate a one common backbone key (i.e. Outer group Key (KG)) headed by the Outer Group Controller using ECTGDH protocol.

3. Each Group Controller (Sub /Outer) distributes the computed public key to all of its members. Each member performs rekeying to get the corresponding shared key..

A Regional key KR is used for communication between a subgroup controller and the members in the same region. The Regional key KR is rekeyed every time whenever there is a membership change event, sub group join / leave and member failure. The Outer Group key KG is rekeyed whenever there is a join/ leave gateway controllers and member failure to preserve secrecy. The members within a subgroup use Elliptic Curve Group Diffie-Hellman Contributory Key Agreement (ECGDH). Each member within a subgroup contributes his share in arriving at the subgroup key. Whenever membership changes occur, the subgroup controller or previous member initiates the rekeying operation.

Algorithm 2. Multilevel Access Control Using ECC

1. **Member Join**

When a new member joins, it initiates communication with the subgroup controller. After initialization, the subgroup controller changes its contribution and sends public key to this new

member. The new member receives the public key and acts as a group controller by initiating the rekeying operations for generating a new key for the subgroup. The rekeying operation is as follows.

New node — Join request → Subgroup Controller

Subgroup Controller — change its contribution and send public key to → NewNode; Acts as → New Subgroup Controller

New Node — puts its contribution to all the public key value & Multicast this public key value to → New Subgroup Controller → the entire member in the subgroup

Each Member put is contribution to the public value & Compute → New Subgroup Key

2. Member Leave:

a) When a Subgroup member Leaves

When a member leaves subgroup to which it belongs the subgroup key must be changed to preserve the forward secrecy. The leaving member informs the subgroup controller. The subgroup controller changes its private key value, computes the public value and broadcasts the public value to all the remaining members. Each member performs rekeying by putting its contribution to public value and computes the new Subgroup Key. The rekeying operation is as follows.

Leaving Node — Leaving Message → Subgroup Controller

changes its private key value, compute the public key value and

Subgroup Controller — Multicast the public key value to → All the remaining Member

Each Member — Performs Rekeying and Compute → New Subgroup Key

b) When Subgroup Controller Leaves:

When the subgroup Controller leaves, the subgroup key used for communication among the subgroup controllers needs to be changed. This Subgroup Controller informs the previous Subgroup Controller about its desire to leave the subgroup which initiates the rekeying procedure. The previous subgroup controller now acts as a Subgroup controller. This Subgroup controller changes its private contribution value and computes all the public key values and broadcasts to all the remaining members of the group. All subgroup members perform the rekeying operation and compute the new subgroup key. The rekeying operation is as follows.

Leaving Subgroup Controller — Leaving Message → Old Subgroup Controller

change its private value,compute the all public key value and

Old Subgroup Controller — Multicast → Remaining Member in the group

Subgroup Member Perform Rekeying and Compute → New Subgroup Key

c) When Outer Group Controller Leaves:

When an Outer group Controller leaves, the Outer group key used for communication among the Outer groups needs to be changed. This Outer group Controller informs the previous Outer group Controller about its desire to leave the Outer group which initiates the rekeying procedure. The previous

Outer Group controller now becomes the New Outer group controller. This Outer group controller changes its private contribution value and computes the public key value and broadcast to the entire remaining member in the group. All Outer group members perform the rekeying operation and compute the new Outer group key. The rekeying operation is as follows.

Leaving Outer group Controller → Leaving Message → Old Outer group Controller

Old Outer group Controller → change its private value,compute the all public key value and Multicast → Remaing Member in the Outer group

Outer group Member → Perform Rekeying and Compute → New Outer group Key

d) When Gateway member leaves

When a gateway member leaves the subgroup, it delegates the role of the gateway to the adjacent member having high processing power, memory, and Battery power and the adjacent member acts as a new gateway member. Whenever the gateway member leaves, all the two keys should be changed. These are

i. Outer group key among the subgroups.
ii. Subgroup key within the subgroup.

In this case, the subgroup controller and outer group controller perform the rekeying operation. Both the Controllers leave the member and a new gateway member is selected in the subgroup, performs rekeying in the subgroup. After that, it joins in the outer group. The procedure is same as member join in the outer group

e) Communication Protocol:

The members within the subgroup have communication using subgroup key. The communication among the subgroup members takes place through the inner class controller.

1. Communication within the Subgroup:

The sender member encrypts the message with the subgroup key (KR) and multicasts it to all members in the subgroup. The subgroup members receive the encrypted message, perform the decryption using the subgroup key (KR) and get the original message. The communication operation is as follows.

Source Member → $^{E}KR_{[Message]}$ & Multicast → Destination Member

Destination Member $^{D}KR_{[EKR[Message]]}$ → Original Message

2. Communication among the Subgroup:

The sender member encrypts the message with the subgroup key (KR) and multicasts it to all members in the subgroup. One of the members in the subgroup acts as a gate way member. This gateway member decrypts the message with subgroup key and encrypts with the outer group key (KG) and multicasts to the entire gateway member among the subgroup. The destination gateway member first decrypts the message with outer group key and then encrypts with subgroup key multicasts it to all members in the subgroup. Each member in the subgroup receives the encrypted message and performs the decryption using subgroup key and gets the original message. In this way the region-based group key agreement protocol performs the communication. The communication operation is as follows.

Source Member $^{E}KR_{[Message]\&Multicast}$ → Gateway Member

Gateway Member $^{D}KR[^{E}KR_{[Message]}]$ → Original

***f)* Users joining the Troop class is shown below**

The Troop User1Joins

User Id: Troop User1 Private Key (nA) = 47568

Public key (A) = g^{nA} = (nA mod p) G = (47568 mod 241) G

- 91 G = (206,121)

Troop User2 Joins

User Id: TUser2 Private Key (nB) = 13525

Public key (B) = g^{nB} = (nB mod p) G = (13525 mod 241) G= 29 G = (29,139)

Finding the Group key after Troop user1 and Troop User2 joined the group

TroopUser1 Calculates the Group key

$Tuser_1$ will get g^{nB} from $TUser_2$ i.e. (29,139) yields 29 Shared key = g^{nAnB}

1.((47568*29)mod 241) G

2. 229 G

3.(155,115)

Troop User2 Calculates the Group key

$TUser_2$ will get g^{nA} from $TUser_1$ i.e. (206,121) yields 91 Shared key = g^{nAnB}

1. ((13525*91)mod 241) G

2.229 G

2. (155,115)

Troop $User_3$ Joins the Group

User Id: TUser3 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 Third Troop User joined the Group

The new $TUser_3$ act as a Group controller.

$TUser_3$ 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 $Tuser_1$ and g^{nAnC} Value to $TUser_2$.

Finding the Group key after three users joined the group

Tuser1 Calculates the Group key

Tuser1 will get g^{nBnC} from $TUser_3$ (GC) i.e. (131,84) yields 174

Shared key = g^{nAnBnC}

= ((47568*174)mod 241) G

= 169 G

= (120,31)

TUser2 Calculates the Group key

$TUser_2$ will get g^{nAnC} from $TUser_3$ (GC) i.e. (147,97) yields64.

Shared key = g^{nAnBnC}

= ((13525*64)mod 241) G

= 169 G

= (120,31)

TUser3 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 TUser3 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 TUser1, g^{nA} Value to TUser2. Using the shares the Group keys are calculated

g) Tree-based Group Diffie-Hellman Protocol

In the proposed protocol (Fig.8), Tree-based group Diffie-Hellman (TGDH), a binary tree is used to organize group members. The nodes are denoted as < l, v >, where 0 <= v <= $2^l - 1$ since each level l hosts at most 2^l nodes. Each node < l, v > is associated with the key K<l,v> and the blinded key BK<l,v> = F(K<l,v>) where the function f (.) is modular exponentiation in prime order groups, that is, $f(k) = \alpha^k \bmod p$ (equivalent to the Diffie–Hellman protocol. Assuming a leaf node < l, v > hosts the member Mi, the node < l, v > has Mi's session random key K<l,v>. Furthermore, the member Mi at node < l. v > knows every key in the key-path from < l, v > to < 0, 0 >. Every key K<l,v> is computed recursively as follows:

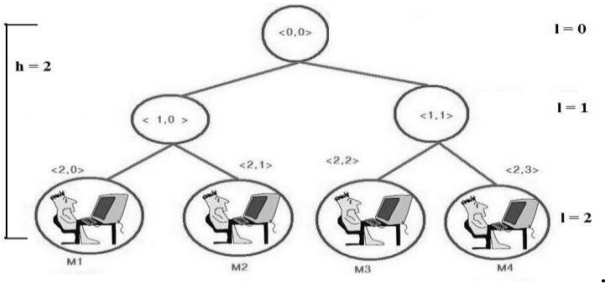

Figure 6. Key Tree

$K<l,v> = K<l+1,2v> BK<l+1,2v+1> \bmod p$

$= K<l+1,2v+1> BK<l+1,2v> \bmod p$

$= K<l+1,2v> K<l+1,2v+1> \bmod p$

$= F(K<l+1,2v> K<l+1,2v+1>)$

It is not necessary for the blind key BK<l,v> of each node to be reversible. Thus, simply use the x-coordinate of K<l,v> as the blind key. The group session key can be derived from K<0,0>. Each time when there is member join/leave, the outer group controller node calculates the group session key first and then broadcasts the new blind keys to the entire group and finally the remaining group members can generate the group session key.

1. PM+KASK = (160,203)

   PM = (160,203) - KASK = (160,203) -21

   = 126– 21 = 105 G => (185,199)i

(2) PM+KASK = (77,145)

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

= 135 – 21 = 114 G => (172,50) r

(3) PM+KASK = (156,10)

= (156,10) -

PM = (156,10) - KASK 21

= 122 – 21 = 101 G => (1,182)e

a..Elliptic Curves used

Troops Class: $y^2 = x^3 - 4 \bmod 211$ at G(2,2)

NSG Class: $y^2 = x^3 + 8x - 2 \bmod 337$ at G(0,311)

Lieutenants: $y^2 = x^3 + 7x + 5 \bmod 563$ at G(1,442)

AIR Wings: $y^2 = x^3 + 5x - 8 \bmod 823$ at G(3,597)

b .Example Message:

Sent....3:Leutanats:TerroristInformation:440:400:487
:137:493:111:355:172:325:238:54:289:325:238:493:11
1:215:36
0:16:73:505:466:505:466:538:236:505:466:293:20:560
:14

8:478:249:

III. RESULTS AND DISCUSSION

The system was developed in Java net beans and run on a network. Some sample output screens are shown in Figure 6 through Figure 10.

Figure 7. Class Join

Figure 7: User Join

Figure 8. Troop User receives message

Figure 9: Air wing User receives message

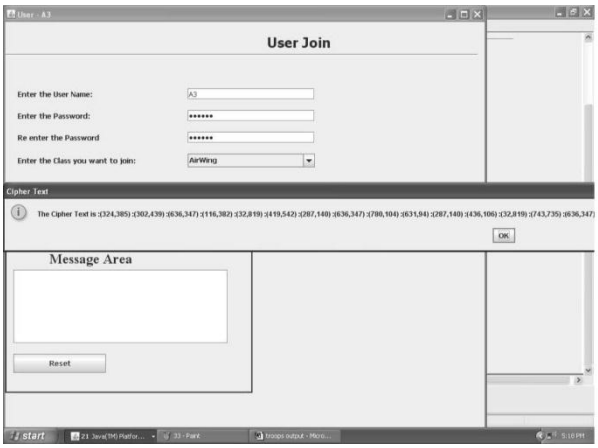

Figure 10: Message gets decrypted

IV. CONCLUSION

We have implemented a Defence Messaging System which is based on Multilevel Access Control Model using Elliptic curve cryptography. We have successfully implemented by selecting different elliptic curves. A single elliptic curve can be used and by changing the generator points we can perform different encryption. The forward and backward secrecy is maintained here. As future implementation, agent based methods can be studied. Thus the members in a particular class are able to receive the messages securely.

V. 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)pp :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 AccessHierarchies", CERIAS Tech Report 2006.

[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,.V.Sumathy, (2009), "A Novel Approach towards cost EffectiveRegion Based Group Key Agreement Protocol for Ad Hoc Networks" ,Intl. Confernce on Computational Intelligence,Communication Systems and Networks ,2009 CICSYN,09 , July 23-25 2009 published in IEEE Explore.

[6] K.Kumar, J.Nafeesa Begum ,.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] R. S. Sandhu. "Cryptographic implementation of a tree hierarchy for access control". Information Processing Letter, 27(2):95.98, Feb. 1988.

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

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

[10] J. Nafeesa Begum, K. Kumar, V. Sumathy, "Design and implementation of Multi-level access Control in Medical Image Transmission using Symmetric Polynomial based Audio Stegnography", (IJCSIS) International Journal of Computer science and Information security.