iJETRM
International Journal of Engineering Technology Research & Management

IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY AND IT'S STUDY FOR SECURE DATA TRANSMISSION IN MULTIPLE ADHOC NETWORKS

Dr. H.V.Kumaraswamy
Rahul R Sherekar
Siddharth Tathagat
R.V. College of Engineering, Bengaluru
kumaraswamyhv@rvce.edu.in
rahulrsherekar@gmail.com
deadpoets77@gmail.com

ABSTRACT

Public-key cryptography has been at the center of online communication and information transfer for decades. With computing power growing at an exponential rate, a number of most widely used encryption schemes are beginning to show their limits. Since these systems may appear on low computing power devices like mobile phones, or chips, it's become essential to make protocols such that we will reach the same level of security without spending considerable computing power putting up the system in the very first place. Elliptic curve cryptography (ECC) provides an exciting alternative to RSA, and has shown to be lot more efficient in terms of key size. Mobile Ad-Hoc Network's (MANET's) is the system, wherein wireless mobile nodes are dynamically self-organized in an arbitrary temporary network topologies that enables people and networks to internetwork with no pre-existing infrastructure. ECC is an alternative mechanism for implementing the public key cryptography and its advantage is that, it has higher efficiency and better scalability. Wireless devices need to utilize Public Key Cryptography in order to improve immunity in security issues such as, authentication, key exchange and it requires a novel solution to overcome them, which are provided by ECC.

KEYWORDS:
Mobile Adhoc Networks (MANETs), Elliptic Curve (EC), Cryptography

INTRODUCTION

Cryptography is the study of various techniques which involves secure transmission of data from a sender to the desired receiver. The techniques differ from each other based on their purpose. Data needs to be protected from several types of attacks during transmission such as brute force attack, replay attack, man-in-the-middle attack, statistical attack, implementation attack, etc. Cryptography includes keys used at both sender and receiver ends to encrypt and decrypt information. Based on keys, it is of two types namely, symmetric key cryptography and public key cryptography. Symmetric key cryptography involves use of the same key at both sender and receiver ends whereas public key cryptography involves use of different keys at sender and receiver ends. A plane curve over a finite field is assumed to be an elliptic curve. Elliptical curve cryptography is a type of public key cryptography. In this type of cryptography, the sender and receiver have a set of public and private keys and the information of how the keys will affect the information during encryption and decryption. All the devices present in this type of communication must know a set of predefined constants such as domain parameters. This type of cryptography has less speed than private key cryptography, but the main advantage is that the key size is small. So, as compared to other algorithms, it can attain the same level of security with smaller keys. Some of the applications of Elliptical curve cryptography are digital signatures, key-agreement and pseudo random generators.

A MANET (mobile ad-hoc network) is a network of mobile nodes that satisfy two purposes – they can act as routers as well as hosts in a wireless network. They have a dynamic self-organizing property without the use of an infrastructure that hasn't been already established. These are used to make tasks more efficient by offering unprecedented information access. Their main characteristics are that they have a dynamic topology and that prediction of frequent changes to topology is hard. They have wireless links as their base because of which they have less physical security. Also, they have lower capacity than those networks which use wired links. A MANET can be formed by two or more users if they are close enough and they meet the radio constraints.

OBJECTIVES

The objective of this work is to study elliptic curve cryptography, implement it using a scalar multiplication method to generate keys, and further study the use of elliptic curve cryptography in the security of mobile adhoc networks.

METHODOLOGY

Key generation using Elliptic Curve Cryptography is implemented. A random value d is chosen by both the receiver and the sender parties such that it lies between 1 and n-1 where n is the prime order of g (generator point). The prime order of g is the smallest number such that n*g is an elliptic identity. Then, a point P is obtained on the elliptic curve which is the multiplication of points d and g, this point is made public. This P value is then exchanged between the two parties. P becomes the public key. Another point R is calculated by the multiplication of points d and P. Now, both parties have the same R, which is then kept private and will further be used for encryption. A method is proposed for security of MANETS. The message is to be constructed and thresholded, and converted to packets. Then, the packets are to be encrypted using Elliptic Curve Cryptography and made ready for forwarding. Then, the encrypted packets are to be forwarded over the network to the receiver. Similar decryption process is to be used at the receiver to reverse the encryption process and obtain the original message.

RESULTS AND DISCUSSION

This section looks into the design and implementation of the Elliptic Curve Based cryptography method to generate keys and also its proposed implementation in security of MANETs. First, we look at the ECC key generation algorithm. The steps for the generation of the public/private key pair are as follows:
1. Each party selects a random value d such that the value of d is between 1 and n-1.
2. d*g = P = (xG, yG) is made public.
3. The two parties then send the P values generated to each other. P is the public key.
4. Then, a third point R = d*P is calculated. R = d * (other d) * G = (xR, yR). So, now both the parties have same coordinates. R is kept private.
5. This R now acts as the private key which is further used for encryption.
Where, p = Field that curve is defined over, (a,b) = Values that define the curve, g = Generator point, n = Prime order of g (smallest number such that n*g = elliptic identity), h = cofactor (number of points over the curve n).
There are several different diagrams which can be used for analysis of the proposed method for securing MANETs:

Class diagram

Class diagrams are the mainstay of object-oriented analysis and design. Class diagrams show the classes of the system, their interrelationships (including inheritance, aggregation, and association), and the operations and attributes of the classes. Class diagrams are used for a wide variety of purposes, including both conceptual/domain modeling and detailed design modeling.

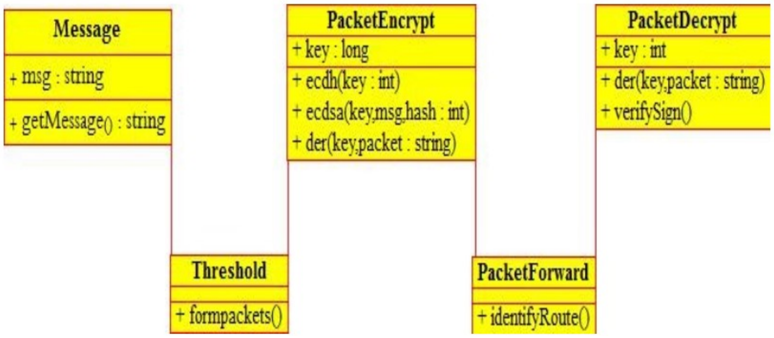


Figure 1: Class Diagram

Usecase diagram

A use case is a set of scenarios that describes an interaction between a user and a system. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors. An actor represents a user or another system that will interact with the system modeled. A use case is an external view of the system that represents some action the user might perform in order to complete a task.

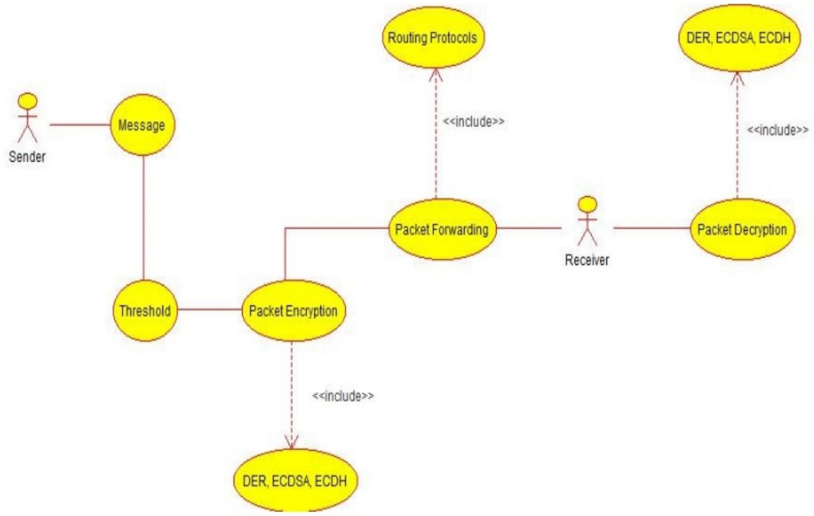


Figure 2: Usecase Diagram

Interaction diagram

A sequence diagram in Unified Modeling Language (UML) is the one interaction diagram that shows how processes operate with each other and in what order. It is a representation of a message sequence chart. A sequence diagram shows different processes or objects that live simultaneously, as horizontal arrows, the messages exchanged between them, in the same order which they occur. This allows the specification of various simple runtime scenarios in graphical manner.

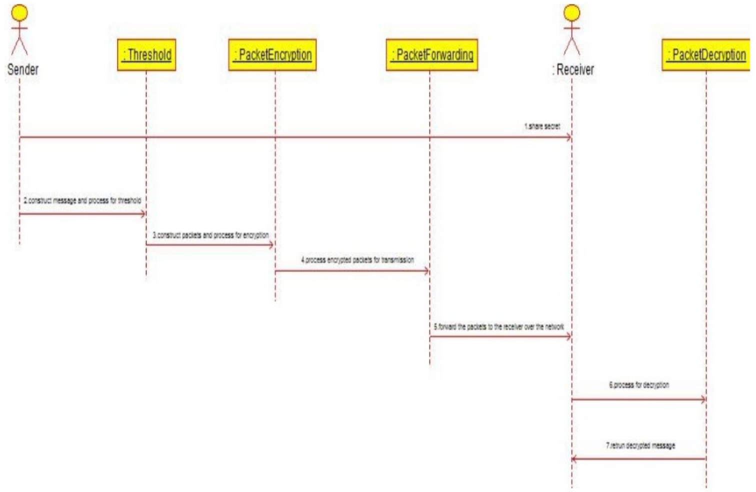

Sender
: Threshold
: PacketEncryption
: PacketForwarding
: Receiver
: PacketDecryption
1.share secret
2.construct message and process for threshold
3.construct packets and process for encryption
4.process encrypted packets for transmission
5.forward the packets to the receiver over the network
6.process for decryption
7.retrun decrypted message

Figure 3: Interaction Diagram

The test cases for ECC-Based Threshold Cryptography for MANET's are identified as follows:

1. Check the possibility for inputting the message which might be numeric, alphabetic or alpha-numeric or any special character.
2. Check what happens if message is processed as void.
3. Check whether the packet formation is based on the code.
4. Check whether the values obtained after encryption vary for different types of inputs.
5. Check what happens if correct transmission is chosen.
6. Check what happens if incorrect transmission is chosen.
7. Check what happens if duplicate packet transmission is chosen.
8. Check whether there is a possibility of discarding the duplicate packets.
9. Check whether there is possibility for the receiver to view the message after the entire process.

Following are the results obtained in the ECC method:

In the general equation for an elliptic curve, y^2 = x^3 + a*x + b, a and b are both taken as '2' and the resulting elliptic curve is shown in the figure.

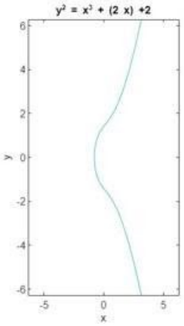


Figure 4: Elliptic curve with a=b=2

Then, the algorithm proceeds and the results of the elliptic curve point multiplication are obtained and are plotted as shown in figure.

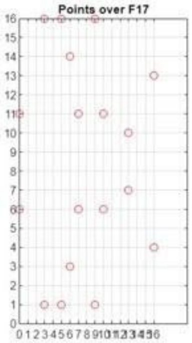
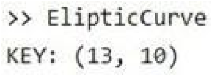


Figure 5: ECC point multiplication plot

Finally, the algorithm is completed and the entire process results in a key generated which is the output of the code.



```
>> ElipticCurve
KEY: (13, 10)
```

Figure 6: Resulting Key

ACKNOWLEDGEMENT

We thank the staff and our colleagues from R.V. College of Engineering, and our guide, H.V. Kumaraswamy, who provided insight and expertise that greatly assisted the research. We are expressing our gratitude to our families for being an inspiration. Above all, to God.

CONCLUSION

In this paper, a demonstration of Elliptic Curve Cryptography has been presented by using the method to create a private/public key pair and how the method can be used in mobile ad-hoc networks to enhance its security is further studied. The security-sensitive applications of ad hoc networks require high degree of security, but ad hoc networks are inherently vulnerable to security attacks. Threshold cryptography is a valid approach to build a highly available and highly secure key management service by distributing trust among a group of servers. Elliptic curve cryptography provides an efficient alternative to other public key encryption algorithms. Elliptic curve digital signature algorithm is highly effective in establishing the legitimacy of the communicating parties and Elliptic curve Diffie-Hellman key exchange scheme on the other provides a secure way of sharing the encryption key between the shared users participating in the communication.

REFERENCES

[1] Kumar, A. Vinodh, and S. Mohideen, "Elliptical Curve Cryptography Algorithm for Secure Mobile Adhoc Network." Journal of Theoretical & Applied Information Technology 77.3 (2015).

[2] Kumar, Rohit, Yashendra Shiv, Vimal Kumar, and Manoj Wairiya, "An authentication technique in mobile Ad hoc network using elliptic curve cryptography." 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2018.

[3] Naveena, A., and K. Ramalinga Reddy. "A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks." ETM Dept, G. Narayanamma institute of Engineering and Technology for Women. International Research Journal of Engineering and Technology (IRJET) Volume 3 (2016).

[4] Bos, Joppe W., et al. "Elliptic curve cryptography in practice." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014.

[5] Papadimitratos, Panagiotis, and Zygmunt Haas. "Secure routing for mobile ad hoc networks." Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002). No. CONF. SCS, 2002.

[6] Koblitz, Neal, Alfred Menezes, and Scott Vanstone. "The state of elliptic curve cryptography." Designs, codes and cryptography 19.2-3 (2000): 173-193.

[7] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.

[8] Johnson, Don, Alfred Menezes, and Scott Vanstone. "The elliptic curve digital signature algorithm (ECDSA)." International journal of information security 1.1 (2001): 36-63.

[9] Kurkowski, Stuart, Tracy Camp, and Michael Colagrosso. "MANET simulation studies: the incredibles." ACM SIGMOBILE Mobile Computing and Communications Review 9.4 (2005): 50-61.

[10] Kumari, Sarita. "A research paper on cryptography encryption and compression techniques." International Journal Of Engineering And Computer Science 6.4 (2017).