ISSN:0975-9646

PKC Based Mutual Node Authentication in Wireless Mesh Network Using ECC Algorithm

Ajit P. Shiralkar [1], Prof. Ranjit R. Keole [2]

[1]*M.E. Scholar (Comp.Sci. & Engg.), H.V.P.M's C.O.E.T. S.G.B.A.U, Amravati, India*
[2]*Lecturer in Dept. Of Information Technology, H.V.P.M's C.O.E.T., S.G.B.A.U, Amravati, India*

Abstract— **Wireless Mesh Networks (WMNs) are new emerging potential for strengthening Internet deployment and access. As WMS is a useful media for a wireless communication between various nodes the Authentication from a Security point of view is required to Improve. A well-performed security framework for WMNs will contribute to network survivability and strongly support the network growth. The secure Key generation is the best solution for creating a Authentication between communicating Nodes. A low-computational and scalable key management model for WMNs is to guarantee well-performed key management services and protection from unauthorized access. The RSA-based protocols have significant problems in terms of the bandwidth and storage requirements.**
With RSA this security can be maintained with the mechanism that Longer the Key generated, more security can be provided. The RSA algorithm requires that the key length be at least 1024 bits for long term security which is not compatible with the Devices having less Storage & Bandwidth. Instead, ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC offers equivalent security with smaller key sizes; these result in faster computations, lower power consumption, as well as memory and bandwidth savings. ECC is especially useful for mobile devices, which are typically limited in terms of their CPU, power and network connectivity however, it seems that 160 bits are sufficient for elliptic curve cryptographic functions. Thus, use of ECC in wireless mesh network ,can improved security substantially.

Keywords— **WMN, PKC, ECC, Cryptograph, RSA.**

I. INTRODUCTION

Wireless Mesh Networks (WMNs) enable wireless communication between infrastructure components of the network. These are new emerging potential for strengthening Internet deployment and access. WMNs thus make an abundance of wires obsolete, leading to a flexible and potentially dynamic network infrastructure. Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes.

They can automatically establish ad hoc networks and maintain mesh connectivity between them. WMN's diversify the abilities of ad hoc networks as they are composed of mesh routers and mesh clients. Mesh clients perform pure ad hoc behaviour by performing routing and self configuration [1], [17].

Wireless Mesh Network is an application technology different from the traditional peer-to-peer wireless bridges it provides the multi-hop and multi-path connection to form a wireless environment of MESH framework so that the occurrence of single point failure can be prevented. There are 3 types of components under the framework of Wireless Mesh Network:

a) MP (Mesh Point): Nodes in the mesh network, in charge of the delivery of the packets from each node.

b) MAP (Mesh Access Point): It works with the functions of middleware transmission in the mesh network.

c) MPP (Mesh Portal) : It plays as the bridge for interfacing two networks, usually connects the wired network with the wireless MESH network

The main difference between mesh clients and mesh routers is that clients only have one wireless interface and less computational abilities. With this infrastructure provides connectivity to other networks, routing abilities of clients provide improved connectivity and coverage within the mesh network. In order to have reliable proper security over the wireless communication channel, certain security measures, e.g. confidentiality, authenticity, and untraceability need to be provided [2].

A critical requirement for the security in WMN is the authentication of a new user who is trying to join the network. In this paper, we present a new authentication scheme based on a combination of techniques, such as zone-based hierarchical topology structure, virtual certification authority (CA), off-line CA, identity-based cryptosystem and multi-signature [3].

For maintaining security in network along with proper authentication PKC is the most useful and reliable method got invented. PKC can be done with many cryptographic algorithms where key storage is constraint, but Elliptic Curve Cryptography can removed this barrier as the RSA algorithm requires that the key length be at least 1024 bits for long term security which is not compatible with the Devices having less Storage & Bandwidth. Instead, ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments where ECC is especially useful for mobile devices, which are typically limited in terms of their CPU, power and network connectivity however, it seems that 160 bits are sufficient for elliptic curve cryptographic functions [12].

II. LITERATURE REVIEW

In 1976, Whitefield Diffie & Martin E. Hellman introduces new Approach for mutual Authentication and for security purpose of Cryptography. Due to PKC i.e Public

Key Cryptography two users who wish to communicate can it is must that they both should have a common key at both the ends [4].

Taher Elgamal, introduces PKC based on Discrete Algorithms in 1985, He stated a public key cryptosystem and a signature scheme based on the difficulty of computing discrete logarithms over finite fields. The systems are only described in GF(p). introduces a new digital signature scheme that depends on the difficulty of computing discrete logarithms over finite fields. It is not yet proved that breaking the system is equivalent to computing discrete logarithms [5].

In 1998, M. Aydos, B. Sunar, and C . K. Koc proposed an authentication and key agreement protocol for wireless communication based on elliptic curve cryptographic techniques. With The use of elliptic curve cryptographic techniques provide greater security using fewer bits, resulting in a protocol which requires low computational overhead, and thus, making it suitable for wireless and mobile communication systems, including smartcards and handheld devices. After defining ECC in Section 3 of their paper they proposed extended work of ECC as Elliptic Curve Digital Signature Algorithm in Section 4 [2].

Kaleemullah Khan, and Muhammmad Akbar in 2006, introduces New methodology for secure authentication technique, with light over-heads that can be conveniently implemented for the ad-hoc nodes forming clients of an integrated WMN, thus facilitating their inter-operability. The proposed authentication scheme is based on using EAP-TTLS (Tunnelled Transport Layer Security) over PANA. EAP-TTLS provides flexibility in using any of the authentication protocols i.e. Password Authentication Protocol (PAP), Challenge Handshake authentication Protocol (CHAP), or Message Digest 5 (MD5) etc. The EAP-TTLS extends EAP-TLS to exchange additional information between client and server by using secure tunnel established by TLS negotiation [6].

In 2009, Ranbir Soram, introduces a New Secure communication model specially for Cellular Communication. He investigated the security loopholes in SMS banking and propose a system to make mobile SMS banking secure using Elliptic Curve Cryptosystem(ECC). His ECC module receives the text messages from the clients/banks and processes them and sends the output back to the banks/users as and when required. This ECC Banking module provides secure data encryption and decryption using public key cryptography .The technology is perfectly secure and GPRS is not mandatory. He introduces ECC Using the real numbers for cryptography have a lot of problem as it is very difficult to store them precisely in computer memory and predict how much storage will be needed for them. The difficulty can be solved by using Galois fields. In a Galois field, the number of elements is finite. Since the number of elements if finite, we can find a unique representation for each of them, which allows us to store and handle the elements in an efficient way. Galois showed that the number of elements in a Galois field is always a positive prime power, pn and is denoted by GF(pn). Two special Galois fields are standard for use in Elliptic Curve cryptography. They are GF(p) when n=1 and GF(2n) when p=2 [7].

R. Rajaram Ramasamy, M. Amutha Prabakar, M. Indra Devi, and M. Suguna in 2009, introduces ECC Algorithm using Knapsack Algorithm. They presented the implementation of ECC by first transforming the message into an affine point on the EC, and then applying the knapsack algorithm on ECC encrypted message over the finite field GF(p). In ECC we normally start with an affine point called Pm(x,y). This point lies on the elliptic curve. In this paper we have illustrated encryption/decryption involving the ASCII value of the characters constituting the message, and then subjecting it to the knapsack algorithm. They compared their algorithm with RSA algorithm and show that our algorithm is better due to the high degree of sophistication and complexity involved. It is almost infeasible to attempt a brute force attack [8].

In year 2012, Peng Xiao, Jingsha H2 and Yingfang Fu proposed effective distributed key management scheme for the establishment of a secure WMN in this paper, which is based on several technologies, such as ad hoc network model, ECC, (t, n) threshold cryptographic, verifiable secret sharing. He introduces the method that all mesh nodes need to acquire a legal certificate from the offline CA, which is supported by an ISP or network carrier [9]. And as there is no CA or administrator center online in the backbone mesh networks, n mesh routers with higher performance will form a virtual CA and group key management (GKM) to manage the keys using the (t, n) threshold cryptographic method [10].

In 2013, Merad BOudia Omar Rafiq and Feham Mohammad had proposed Fast & Secure Implementation of ECC algorithm using Concealed Data Aggregation. Because of which a System just needs 1.29 seconds for encryption & Decryption as well [10].

In 2014, Ravi Kishore Kodali introduces Implementation of ECC with Hidden Generator Point in Wireless Sensor Networks. He proposes a technique for ECC with a hidden generator point in order to overcome the MIM (Man In Middle) attack. He used Three different algorithms based on distribution of points on the elliptic cure (EC), using a different generator point for each encrypted message and selecting different generator points for each session are discussed[11].

III. PROBLEM ANALYSIS

Wireless Mesh Networks, an emerging technology, are considered as the promised choices for wireless Internet communications since they allow fast, easy, and low-cost network deployment [12]. The nature of flexible dynamic deployment and the lack of the fixed infrastructure expose WMNs to suffer varieties of security attacks as various applications of Wireless Mesh Networks have been explored, the security mechanisms are unfortunately unexplored. All the current security mechanisms (e.g. encryption, digital signature and authentication) which can be used for WMNs are based on cryptographic keys and thus high degree key management services are in demand.

A well-performed security framework for WMNs will contribute to network survivability and strongly support the

network growth. The secure Key generation is the best solution for creating a Authentication between communicating Nodes. A low-computational and scalable key management model for WMNs is to guarantee well-performed key management services and protection from unauthorized access. The RSA-based protocols have significant problems in terms of the bandwidth and storage requirements. With RSA this security can be maintained with the mechanism that Longer the Key generated, more security can be provided. The RSA algorithm requires that the key length be at least 1024 bits for long term security which is not compatible with the Devices having less Storage & Bandwidth.

Instead, ECC is more and more considered as an attractive public-key cryptosystem for mobile/wireless environments [7]. Compared to traditional public-key cryptosystems like RSA or Diffie-Hellman, ECC offers equivalent security with smaller key sizes; these result in faster computations, lower power consumption, as well as memory and bandwidth savings.

IV. EXISTING METHODOLOGY OF ECC ALGORITHM

ECC can be used for providing the following security services: confidentiality, authentication, Data Integrity, Non repudiation, Authenticated key exchange.

The elliptic curves are suitable in applications where: The computing power is limited (intelligent cards, wireless devices, PC boards); Memory size on integrated circuit is limited; A great speed of computing is necessary; Digital signing and its verification are used intensively; Signed messages have to be transmitted or memorized; Digital bandwidth is limited (mobile communications, certain computer networks) [7].

From the advantages of ECC usage, there can be mentioned:

- Increased security: cryptographic resistance per bit is much greater than those of any public-key Cryptosystem known at present time;
- Substantial economies m calculus and memory needs in comparison with other cryptosystems;
- Great encryption and signing speed both in software and hardware implementation;
- ECC is ideal for small size hardware implementations (as intelligent cards);
- Encryption and signing can be done in separate stages.

Elliptic curves are mathematical constructions. An elliptic curve can be defined over any field (of real, rational or complex numbers), but – generally speaking - the elliptic curves used in cryptography are defined over finite fields.

An elliptic curve consists of the points satisfying the equation:

y^2=x^3+ax +b

Where x, y, a and b are elements in GF (q) (a Galois Field of order, where is a prime).

Each choice of (a, b) yields a different elliptic curve.

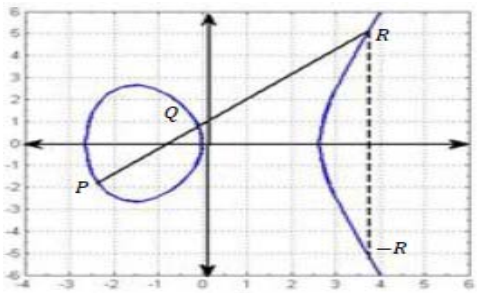

Fig. 1 An Elliptic Curve obtained with Algorithm

P (-2.35,-186)

Q (-0.1, 0.836)

-R (3.89,-5.62)

P+Q=R= (3.89,-5.62)

$y^2 = x^3+7x$

The elliptic curve group operation is closed under addition so that addition of any two points is also a point in the group. Given two points P (x_1, y_1) and Q (x_2, y_2) , the addition results in a point R (x_3, y_3) given by:

$(x_1, y_1) + x_2, y_2) = (x_3, y_3)$

Such that

$x_3 = \beta 2 + \beta + x_1 + x_2 + a$

$y_3 = \beta (x_1 + x_3) + x_3 + y_1$

$\beta = (y_1+y_2) / (x_1 + x_2)$

An example of P (-2.35,-186) and Q (-0.1, 0.836) is illustrated in Figure 1.

If P=Q, then R = P+P=2P. Addition of multiple points will give. ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), that is, given points P and Q of the group, it is practically infeasible to find a number K such as .Q=k × p.

The following algorithm gives the points on the curve Ep(a,b).

```
Algorithm elliptic_points(p,a,b)
{
        x=0
        while(x<p)
        {
        w=(x3+ax+b) mod p
        if( w is a perfect square in Zp )
        output ((x,sqrt(w)),(x,-sqrt(w)))
        x=x+1
        }
}
```

With this algorithm the key management with ECC can be done for mutual authentication in WMN. Through the software using simulator these key generations and node authentication can be easily implemented to prove the ECC Algorithm for public key generation [7], [13], [1].

V. PROPOSED WORK

In WMN, for secure communication in different nodes confidentiality, authenticity, and untracebility are the required factors. PKC is the solution through which communication can be made secure and fruitful.

PKC can be made through various methods, among all these ECC can be implemented for faster and most secure key generation and proper authentication. With the help of this Elliptic Curve Cryptography methods the key can be get generated and security can be maintained at fastest and with low space consumption. This algorithm can be implemented on simulator and key generation as well node authentication in WMN can be shown.

VI. CONCLUSIONS

In this world of technology peer to peer communication is Very essential area as more and more applications are coming out, the destination of this promising technology, saying WMNs, will be well-performed, secure, and wide-spread wireless connection. This paper can be used to give a baseline for building a tight security for wireless mesh networks. Public-key cryptography is feasible for wireless mesh network security applications including access control. With more and more applications coming out, the destination of this promising technology, saying WMNs, will be well-performed, secure, and wide-spread wireless connection. ECC-based access control scheme in wireless mesh network the protocol for the network to authorize a user to access the network. Implementation of ECC on primary field performance will increase substantially. In future it is possible to further reduce the running time by using more refined and careful programming. Public-key cryptography is feasible for wireless mesh network security applications including access control.

REFERENCES

[1] Ion TUTANESCU, Constantine ANTON, University of Pitesti, ROMANIA, *Elliptic Curve Cryptosystem Approaches*, IEEE, 2012..

[2] M. Aydos, B. Sunar, and C. K. Koc, *An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication*, 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October 30, 1998..

[3] Yingfang Fu, Jingsha He, Rong Wang, Guorui Li, *Mutual Authentication in Wireless Mesh Networks*, IEEE, 2006.

[4] Whitefield Diffie & Martin E. Hellman, *New Directions In Cryptography*, IEEE, 1976.

[5] Taher Elgamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE, 1985.

[6] Kaleemullah Khan, and Muhammmad Akbar, *Authentication in Multi-Hop Wireless Mesh Networks*, World Academy of Science, Engineering and Technology 22 ,2006.

[7] Ranbeer Soram, *Mobile SMS Banking Security Using Elliptic Curve Cryptosystem*, International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[8] R. Rajaram Ramasamy, M. Amutha Prabakar, M. Indra Devi, and M. Suguna, *Knapsack Based ECC Encryption and Decryption*, International Journal of Network Security, Vol.9, No.3, PP.218–226, Nov.,2009.

[9] Peng Xiao, Jingsha H2 and Yingfang Fu, *Distributed Group Key Management in Wireless Mesh Networks*, International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[10] Merad BOudia Omar Rafiq and Feham Mohammad, *Fast & Secure Implementation of ECC Based Concealed Data Aggregation in WSN*, IEEE, 2013.

[11] Ravi Kishore Kodali, *Implementation of ECC with Hidden Generator Point in Wireless Sensor Networks*, IEEE, 2014.

[12] Li Gao, Elizabeth Chang, Sazia Parvin, Curtin University of Technology, Australia, *A Secure Key Management Model for Wireless Mesh Networks*, IEEE, 2010.

[13] Avinash Wadhe, N.A.Chavhan, Nagpur, *Practical Approach for Improving Security in Wireless Mesh Network Through ECC and Two Way Authentication Scheme*, International Journal of Computer Applications, 2012.