# Node Authentication using Elliptic Curve Cryptography in Wireless Mesh Network

**Ram Deshmukh[1], Dr.M.A.Pund[2]**

[1]*Student, Department of Computer Science and Engg., Prof. Ram Meghe Institute of Technology & Research*
[2]*Prof., Department of Computer Science and Engg., Prof. Ram Meghe Institute of Technology & Research*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract –** *Wireless Mesh Network is one of the most important network which is self organize and multi hop network. Any node of the network transfer data to any other node in the network so data of the network is less secured. Algorithm like Rivest, Shamir and Adleman (RSA) Algorithm and Advance Encryption Algorithm (AES) are used. It has required high space so it is harder to implement where the authenticity of the message pass from one node to other with limited memory and need higher security. Elliptic Curve Cryptography (ECC) is the best option for less memory and high security. ECC is more effective authentication perform with Elliptic Curve Digital Signature Algorithm (ECDSA). Data transfer along with key more secure and provide data to authenticated node.*

***Key Words***: ECC, Wireless Mesh Network, ECDSA.

## 1. INTRODUCTION

Wireless Mesh Networks (WMN) is widely used one of the most important technology for the twenty-first century which is developed on the basis of WLAN and Ad-Hoc. Compared with the general wireless networks, Wireless Mesh Network has a stronger compatibility to support more types of networks, and the difference is that its backbone nodes are generally static with the Ad-Hoc, that is to say, it's topology is relatively stable.[1] WMN is widely used in Metropolitan Area Network broadband access, Campus Network and Tourism and leisure sites for the advantage of high reliability, spectrum efficiency and compatibility. It is gaining possible attention as a possible way for Internet service providers and other end-users to establish robust and reliable wireless broadband service access at a reasonable cost.

Different from traditional wireless networks, nodes in WMN automatically establish and maintain network connectivity. This feature brings many advantages for the end-users, such as low up-front cost, easy network maintenance, robustness, and reliable service coverage [3]. The gateway and bridge functionalities in mesh routers enable the integration of wireless mesh networks with various existing wireless networks, such as wireless sensor networks, wireless-Fidelity (Wi-Fi), and WiMAX [1].

In wireless mesh network which contains a number of nodes which involves the node to node message transfer with multi hop protocol method of transmission of message from one node to other by means of hop from one node to the other. To ensure that the message is from that particular node to make sure need the Digital signature method. ECDSA play a central role in modern cryptosystems. The basic objective of a digital signature is to guarantee authenticity, integrity of a signed message which is transmitted to the receiver and to prove the identity of the transmitter, including no repudiation. ECC offers shorter signatures compared to other methods as RSA (Rivest Shamir Adleman). This characteristic make ECC suited for applications on constrained devices. ECDSA is generated in three steps; key pair generation, signature generation and the signature verification. Basic blocks in the ECDSA are PRNG (Pseudo-Random Number Generators) for secret key, public key generator by elliptic curve point multiplication and HASH to obtain the condensation of message.

## 2. RELATED WORKS

Efficient key establishment and mutual authentication is important in providing MC seamless roaming and secured access to a WMN. Li, X. Xin and Y. Hu, [7] proposed a symmetric authentication scheme for multi hop WMN, which is based on EAP-TTLS (Tunneled Transport Layer Security). Fitzek et al. Describe an application scheme of IEEE 802.1x in combination with UMTS-AKA to enable authentication and security in IP based multi hop networks. To decrease the authentication delay, Hur et al. [proposed a pre-authentication scheme in a proactive way. To improve the security of authentication process in a multi hop topology, Zhou et al. [5] proposed a mesh certificate based on computationally expensive public key encryption. To provide protection against cloning attack and replay attack, Tang et al. proposed a trust-delegation based efficient mobile authentication scheme (EMAS) based on the elliptic curve discrete logarithm problem. Lee et al. proposed a distributed authentication method which is aimed at decreasing the authentication delay, in which multiple trusted nodes are distributed over the WMN to serve the role of authentication server.

A solution based on the ID-based cryptography is proposed by Zhang et. al [5], which features a novel user broker-operator trust model. To provide better support for fast handover among APs maintained by multiple operators, Bosheng Zhou*, et. al. [21] proposed two certificate-based authentication schemes. Yingfang Fu, et al. [6] proposed an accountable security framework with a sophisticated user privacy protection model based on a short group signature scheme. ZHAI Min, HUANG Ting-Ieicode [5] proposed Public key infrastructure and Certificate authority (CA) which are two very important authentication mechanisms. Because the wireless mesh network does not have pre-established trusted network architecture, therefore, it is unrealistic to establish a central centralized CA[4]. Many scholars have studied and discussed on this issue and advanced many schemes for establishing a distributed CA and key management algorithm based on threshold Cryptography theory, which is used to build distributed CA. and selection standards that are selecting physically and relatively safe nodes and high calculation ability ones as service nodes. Fully distributed CA key management.

## 3. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication [8]. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography. The mathematical operations of ECC is defined over the elliptic curve **y2 = x3 + ax + b,** where **4a3 + 27b2 ≠ 0**. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC.

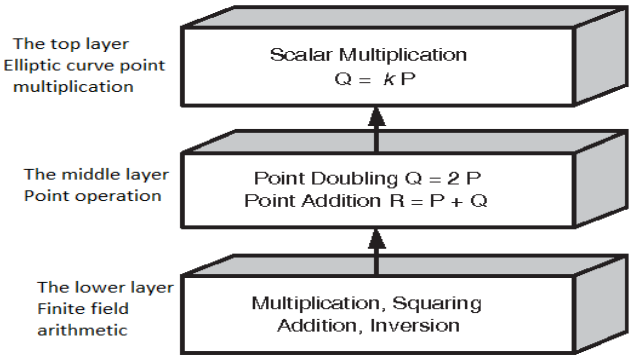


**Figure -1**: Arithmetic Hierarchy

Elliptic curve operation can be performed according three layers, in a hierarchical way. At the top layer, the point multiplication is independently of the selected finite field. This operation is the result of adding the point P to itself (n-1) times. That is K.P=P+P+P+...+P, K times. It can be performed using two kinds of sums for the middle layer: point addition, which consists of the sum of two different points (P + Q) and point doubling, which consist of the sum of the same point (P + P). At the lower layer is the finite field arithmetic. The operators are multiplication, inversion, squaring and adding. The performance of the arithmetic units influences the overall performance of the point multiplication and hence the performance of the ECC cryptographic schemes.

## 4. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

Elliptic curve digital signature allows a sender to generate a signature on a message. The receiver can verify the authenticity of the signature to ensure that the message indeed originated from the claimed sender and has not been modified since. The signature is generated using a private key known only to the sender and verified using a public key known publicly to everyone including the receivers. An adversary cannot forge a sender's signature without the sender's private key.
The signature verification is the counterpart of the signature computation. Its purpose is to verify the message's authenticity using the authenticator's public key. Using the same secure hash algorithm as in the signature step, the message digest signed by the authenticator is computed which, together with the public key and the digital signature components r and s, leads to the result.

### 4.1 Generate Key Pair

Key Pair Steps:
Step 1: Select an elliptic curve E
Step 2: Select a point P from the curve with order n.
Step 3: Choose an integer d from [1, n-1].
Step 4: Compute Q = dP.
P is the point generator of the curve, d is called the private key and Q is the public key.

### 4.2 Generate Signature using Generation Scheme

Signature Generation Steps:
Step 1: Choose an integer k from [1, n-1]
Step 2: Compute k*P = (x1, y1)
Step 3: Compute r = x1 mod n
Step 4: Compute e = h (m)
Step 5: Compute s = $k^{-1}$(e + dr) mod n
Step 6: The signature is the set (r, s).

### 4.3 Perform Signature Verification

Signature Verification Steps:
Step 1: Compute e = h (m)
Step 2: Compute u1 = e$s^{-1}$mod n
Step 3: Compute u2 = r$s^{-1}$mod n
Step 4: Compute u1P + u2Q = (x2, y2)
Step 5: Compute v = x2 mod n
Step 6: The receiver must compare v and r. If v = r then the signature is valid else it is invalid.

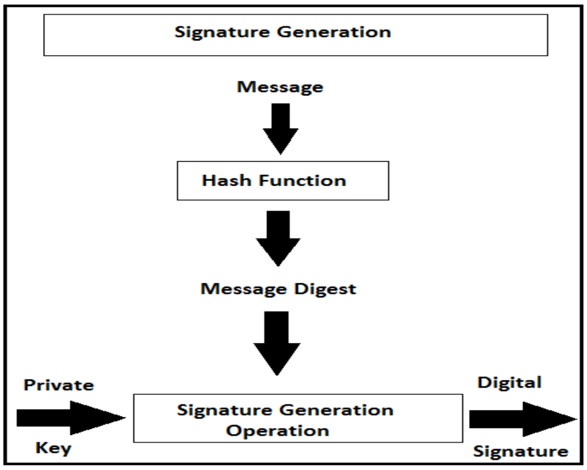


**Figure -2**: Signature Generation

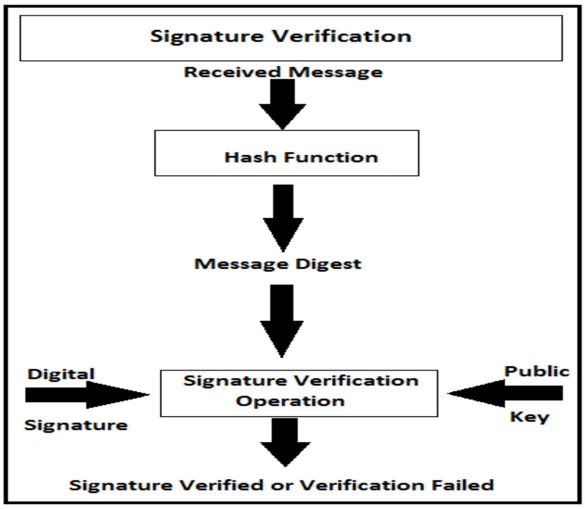
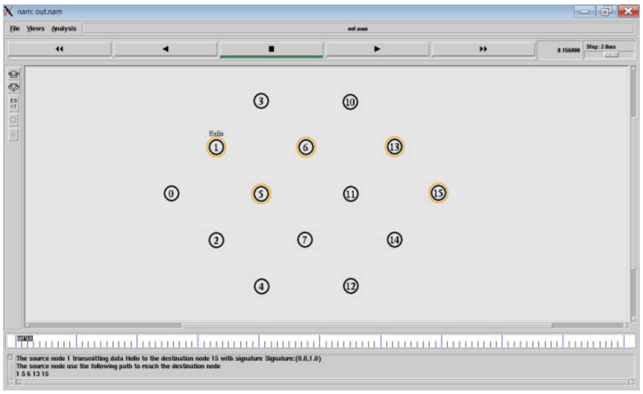


**Figure -3**: Signature Verification

## 5. SIMULATION AND PERFORMANCE ANALYSIS

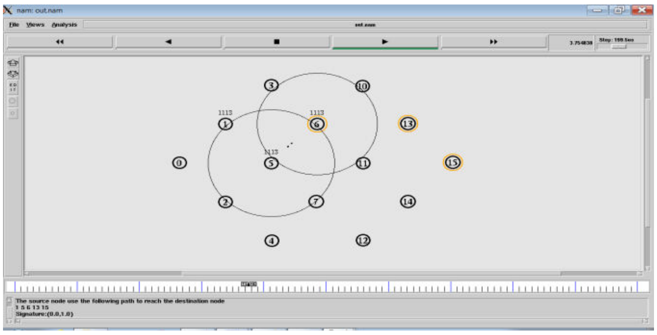
Performance measures of the algorithm are done with the implementation of the concept in network simulator. This gives the results of the better suited approach. In the following experimentation of this implemented algorithm which analyzed based on the computational time and packet transfer delay.
Establishment of a network environment of nodes we have to identify the path from the source to destination node.



The source node 1 transmitting data Hello to the destination node 15 with signature Signature:(0.0,1.0)
The source node use the following path to reach the destination node
1 5 6 13 15

**Figure -4**: Select Path from Source Node to Destination

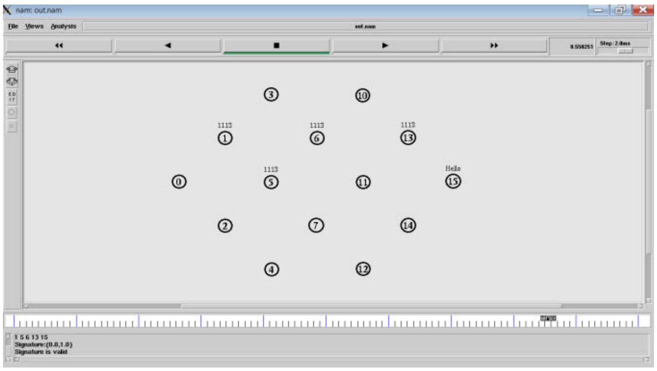
This simulation is shown the forwarding packet through intermediated node.



The source node use the following path to reach the destination node
1 5 6 13 15
Signature:(0.0,1.0)

**Figure -5**: Forwarding Packets

Verify the message authenticity using the authenticator's public key. Using the same secure hash algorithm as in the signature step the message digest signed by the authenticator is computed which, together with the public key and the digital signature components leads to the result. Signature is verified then shown the message which is sender sends to the receiver.



1 5 6 13 15
Signature:(0.0,1.0)
Signature is valid

**Figure -6**: Signature Verification by Destination Node

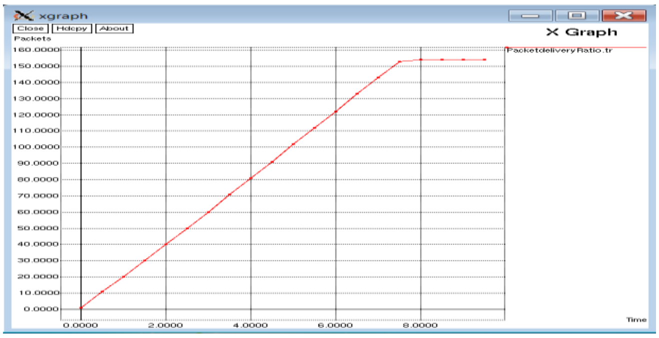


**Figure -7**: Packet Delivery Ratio

Thus we tested node authentication using message in the Network simulator. Figure shown the packet delivery of the networks.

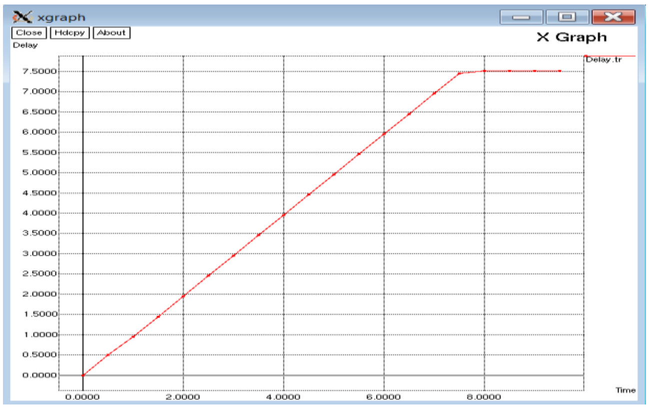


**Figure -8**: Packet Latency Ratio

Latency is a measure of delay. In a network, latency measures the time it takes for some data to get to its destination across the network.

## 6. CONCLUSIONS

As large demands of security features needed in low key size for the Wireless mesh networks ECC has attracted much attention as the security solutions for wireless networks due to the small key size and low computational overhead. Implementation of ECDSA will increase performance of authentication mechanism. Wireless source node forwards the message to the destination node it performs the authentication operation in minimum key size.

## REFERENCES

[1] Yatao Yang Ping Zeng Xinghua Yang Yina Huang (2010),"Efficient Intrusion Detection System Model in Wireless Mesh Network" Second International Conference on Networks Security, Wireless Communications and Trusted Computing.

[2] Jinyuan Sun, Chi Zhang (2011), "SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks" IEEE transactions on dependable and secure computing, vol. 8, no. 2.

[3] Ghanmy Nabil and Fourati Lamia, "Hardware implementation of Elliptic Curve Digital Signature Algorithm (ECDSA) on Koblitz Curves ,"PP.4577-1473 3/12/2012IEEE.

[4] Jinyuan Sun and Chi Zhang,"A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks"Proceeding of IEEE Transactions on Dependable and Secure Computing vol 8, No.2,PP 1545-5971/2011.

[5] ZHAI Min and HUANG Ting-lei,"A RSA Keys Sharing Scheme based on Dynamic Threshold Secret Sharing Algorithm for WMNs," 2010IEEE.

[6] Yingfang Fu and Jingsha He, "Mutual Authentication in Wireless Mesh Networks"Proceeding of IEEE Transactions on Dependable and Secure Computing vol8 No.2,1545-5971/2011.

[7] Pravin Raj.S and A Pravin Renold,"An Enhanced Elliptic Curve Algorithm for Secure Data Transmission In Wireless Sensor Network"Proceeding of 2015 Global Conference on Communication Technologies(GCCT 2015) 978-1-4799-8553-1/2015 IEEE.

[8] Aqeel Khalique and Kuldeep Singh, "Implementation of Elliptic Curve Digital Signature Algorithm" International Journal of Computer Application(0975-8887) Volume 2-No.2, May 2010.

[9] Leonardo B. Oliveira and Aman Kansal, "Secure-TWS: Authenticating Node to Multi-user Communication in Shared Sensor Networks" The Computer Journal, volume 55 No.4,2012.

[10] Jian Li, Yun Li, Jian Ren, Senior Member, IEEE, and Jie Wu,Fellow(2014)," Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks", IEEE, Vol 25, pp.1223-1232.

[11] Liu Z, Wenger E, and Grobschadl j.(2014),"MoTE-ECC:Energy-scalable elliptic curve cryptography and Network Security",pp.361-379.

[12] M A Pund and S S Dandge,"An Overview of Cloud Computing: Platforms,Security Issues and Application", International Journal(IJSTMR),2017,Vol-2,Issue-5.

[13] E-book -Cryptography and Network Security by William Stalling.

[14] E-book-Advances In Elliptic curve cryptography by londan mathematical society.