authenticated else system is completely broken since the polynomial is fully recovered.

3. Objective of Proposed Work

Each message is transmitted along with the digital signature of the message using sender's private key in public –key based approach. Using sender's public key final receiver and intermediate forwarder can authenticate the message. In recent studies in ECC shows that public key is advantageous in terms of computational complexity ,resilience, simple approaches. So we propose an unconditionally secure SAMA based on modified ECDSA scheme. This method is simple It is employed in field arithmetic and elliptic curve arithmetic. It requires little resources and memory.

Here the corrupted message is detected and dropped by the intermediate node so that message is authenticated and sensor power is conserved. Our scheme provides resiliency, flexible-time authentication and source identity protection .It offers no threshold limitation. Both theoretical and simulation analysis demonstrate that proposed scheme is more efficient than Modified Elgamal Signature (MES) and polynomial based algorithms.

Major contributions regarding the paper are as follows:

1. An unconditional source anonymity can be provided by developing a source anonymous message authentication code on elliptic curves.
2. For WSNs an efficient hop-by-hop message authentication mechanism can be offered without threshold limit.
3. In WSNs network implementation criteria on source node privacy protection is devised.
4. For the isolation of compromised nodes an efficient key management framework is proposed.

3.1Recent Developments in the Area

MANETS are collection of mobile nodes which is self creating, self-configuring and self healing without a fixed infrastructure. Each device change the links frequently since it is free to move independently. To provide protected communication in wireless environment security has become a primary concern. By implementing confidentiality using digital signatures and data integrity using hash function mechanisms on hop to hop basis. Elliptic curve cryptography is used to generate digital signatures. By introducing a new routing protocol called Elliptic Curve Cryptography Enabled AODV (ECCEA) as conventional Ad-hoc-On-Demand Distance Vector (AODV) routing protocol development is made to find a solution for this challenge

WSNs when placed in hostile environments are susceptible to various attacks. Key exchange mechanism, handshake protocols are the security and authentication mechanisms. Triple key based broadcast authentication works on Elliptic Curve Diffie- Hellman key agreement scheme. Compared to other security schemes research on WSN authentication performs better.

4. Preliminary Work

An unconditionally secure and efficient anonymous message authentication scheme based on Modified ElGamal Signature scheme on elliptic curve is proposed. It is secure against random oracle model. Here the corrupted message is detected and dropped by the intermediate node so that message is authenticated and sensor power is conserved.

4.1Modified Elgamal Scheme On Elliptic Curves

Let p>3 be an odd prime .An elliptic curve is defined by

$$y^2 = x^3 + ax + bmodp \quad (1)$$

where a,bε f.A special point 0 is at the infinity. Let

G= (x_G , y_G) be the base point on the curve. A selects a random integer d_A ε (1,N – 1) as private key then compute public key as Q_A =d_A ×G.

Signature generation algorithm : To sign a message Alice follows the step

1) A random integer K_A is selected 1 ≤ K_A ≤ N -1
2) r =x_A mod N is calculated. If r=0,go back to step 1.
3) Calculate h_A ,where h is a cryptographic hash function.
4) Calculate s = r $d_A h_A$+K_A mod N,if s=0,go back to step 2.
5) The signature is the pair(r,s).

Signature verification algorithm: To authenticate Alice's signature, Bob must have the public key. Checks Q_A= O.otherwise invalid. Checks nQ_A = O .

1) Verify r,s are integers in (1,N-1).if not signature is invalid.
2) Calculate h_A and(x_1, x_2) = s G −$h_A Q_A$ r mod N.
3) The signature is valid if r =x_1 mod N.invalid otherwise.

5. Design of Proposed Scheme

The proposed authentication scheme aims at achieving the goals.

- **Message authentication**: The receiver should be able to verify that message is send by the claimed node in that particular group.
- **Message integrity**: The receiver should be able to verify whether adversaries modify the message content.
- **Hop-by-hop message authentication:** Authenticity and integrity of the message should be able to be verified by the forwarder on the routing path.
- **Identity and location privacy:** Message sender's ID and location cannot be determined by the adversaries.
- **Node compromise resilience:** It should be resilient to compromised node.
- **Efficiency:** It is efficient in terms of computation and communication overhead.

Here in this block diagram first node is initialized .Then hash function is implemented to convert message to fixed length where intruders may not know thus preventing from intruders. Then we apply verification process .If the verification is success then we transmit message to another node or else that particular node is rejected. Thus saving power resource.