International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Elliptical Curve Cryptography Based Hop-Hop Message Authentication

Devi Radhakrishnan[1]

[1]M.tech student, Department of Electronics and Communication Engineering, Mount Zion College of Engineering, Kadammanitta, Pathanamthitta, Kerala, India

Abstract: ***Sensor networks are implemented in those environment which are always unattended. Thus these networks become vulnerable to intruders. Many standard authentication schemes are implemented to prevent these attack. To reduce the unauthorized attack and malicious access from being forwarded in wireless sensor network message authentication is one of the prominent technique. Many of these techniques are based on symmetric key cryptography and public key cryptography. This method has high computational overhead ,lack of scalability and resilience to node attack. To overcome this advantage in this paper we proposed a source anonymous message authentication scheme (SAMA)based on modified elliptic curve digital signature scheme. This method is better than polynomial based scheme and modified Elgamal signature method(MES).This method allows no threshold to the message transmitted .***

Keywords: Ambiguity set, SAMA, Security server, anonymous, MES

1. Introduction

Message authentication is one of the important method that plays a role in reducing corrupted and unauthorized message being forwarded in WSNs. Because of this reason many message authentication scheme has been developed to provide security and integrity in WSNs. Two approaches are using this techniques and they are symmetric key approach and public-key based approach.

In symmetric key approach it requires complex key management, lacks scalability, not resilient to large no of compromised nodes. The sender uses the shared secret key to generate MAC for each transmitted message. These shared key is shared by group of sensor nodes. Authenticity and integrity of the message can be verified by the node with the help of this shared key. An intruder can compromise the key.

A secret polynomial based message authentication scheme was introduced to solve the scalability problem. It is based on threshold values and its value depend on degree polynomial. When the number of messages transmitted is greater than threshold values messages cannot be transmitted. An alternative solution is to compute coefficients of polynomial. Here we add a random noise called perturbation factor..Hence coefficients of polynomial cannot be easily solved. This random noise can be easily solved by error coding techniques in recent studies.

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.

2. Motivation and Related Works

For achieving security in sensors networks attacking cryptographic scheme [1] shows attack on several cryptography .These schemes use perturbation polynomial in polynomial based system to offer information theoretic security .These scheme is completely broken if the parameters is beyond the above mentioned schemes.

On comparison between symmetric –key and public –key based schemes in [2] system proposed that public key security scheme is more advantageous in many terms like security resilience, memory usage, message complexity.

In paper [3] a random noise factor called perturbation factor is added to the polynomial with a threshold limit. Thus it make difficult for intruders to compute coefficients of polynomial. Recent studies show that using error correcting code techniques perturbation factor can be removed.

False reports can be detect and drop [4] Statistical En-route Filtering (SEF).For en route detection of false report a key assignment method is designed. For enrol report, collective data report generation, filtering and sink generation a mechanism is devised.

In paper[5] for perfect authentication an interleaved hop-hop authentication scheme is purposed .False injection attack is the focus of the author here. Compromised node is filtered out before reaching the base station. Security is the main intention of the author while transmission of packets.

TESLA and EMSS are the efficient schemes introduced in efficient authentication over lossy channel [6] paper .Timed Efficient Stream Loss-tolerant Authentication(TESLA) provide high scalability, minimal overhead, sender authentication. Efficient Multi-chained Stream Signature (EMSS) offers delayed verification, low overhead, high loss resistance.

David Point Cheval and Jacques Stern introduced a signature scheme [7]. This signature scheme is a security proof for random oracle model.

Information- theoretic security in [8] offers threshold limit which is determined by the degree of the polynomial. If the number of messages is less than threshold message is

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.

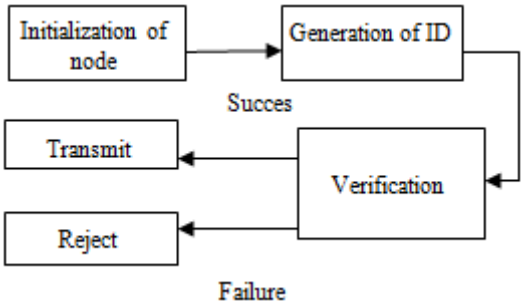

Figure 1(a): Design of proposed system

5.1Proposed Modified Elliptical Curve Digital Signature

Algorithm

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

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

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).

Accelerated ECDSA signature verification:
Input: Signature (r,s) ,message mε{0,1},public key QεG.
Output: Acceptance or rejection of signature relative to Q

Action

1) Verify whether r and s are integers in the interval [1,N-1] its failure leads to rejection of signature.
2) Compute the set of points φ(r)={(x,y)εG| f(x)=r}.
3) Determine set of points R=φ(r).
4) Compute e= H(m).
5) Select an arbitrary point R.
6) Compute S = (v · es^{-1})G + uQ – vR.
7) If S=0, accept signature otherwise reject signature.

5.2 Proposed SAMA On Elliptic Curve

Suppose the sender wishes to transmit a message m anonymously to other nodes. The ambiguity set includes S=(A_1 , A_2, …. , A_n),There is no distinguish between node $A_i$and its public key Q_i.Therefore S = (Q_1 , Q_2 …. , Q_n). Authentication generation algorithm : If m is the message to be transmitted. The private key of the sender is d_A, 1≤t ≤N.

To generate efficient SAMA sender performs the following step

1.Select a random k_i and compute r_t.
2.Finally compute s.

The SAMA of the message m is defined as:

S(m) = (m ,S ,r_1 , y_1 , …. , r_n , y_n).

Verification algorithm: To verify SAMA S(m) = (m ,S ,r_1 , y_1 , …. , r_n , y_n) receiver must have the copy of the public keys (Q_1 , Q_2 …. , Q_n).

6. Features of Proposed Method

6.1 AS Selection And Source Privacy

The source node elects an AS from the public key list before a message is transmitted. This set include itself and some another nodes. When an intruder receives the message he can find the direction of previous hop but he cannot distinguish whether this node is source node.

Some criteria for selecting AS are:

- Message source privacy can be provided by including nodes from opposite direction of the successor node. So that immediate successor cannot distinguish source node and forwarder.
- For energy efficiency nodes should be excluded from the AS that may not be able to add ambiguity.
- Select the nodes within a predefined distance to balance the source privacy and efficiency.
- All the nodes in that range are not included in the AS.

6.2 Key management And Compromised Node Detection

There is an assumption that SS have the responsibility of public-key storage and distribution in WSNs.SS will never be compromised. Sensor node may be compromised by the attackers. These nodes is not able to create public keys that can be accepted by SS.If compromised nodes sends one message it is difficult for sink node to identify it. As more message is transmitted more easily the identification.

In this figure if only one message is transmitted sink node confirms source node in set AS_1.If three messages are send source node will be in shaded area then it is isolated.SS remove public key from its public key list if the node is compromised

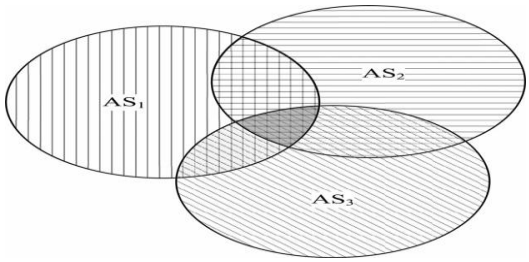

Figure 2(a) : Compromised node detection

7. Simulation Result

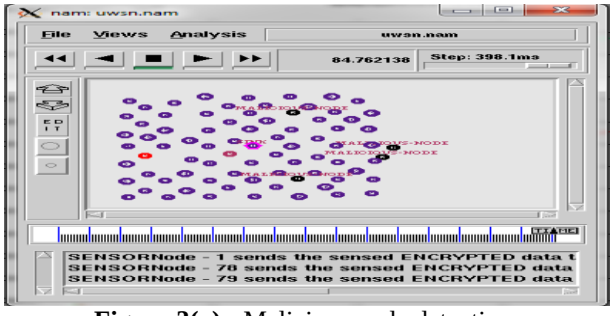

Figure 3(a): Malicious node detection

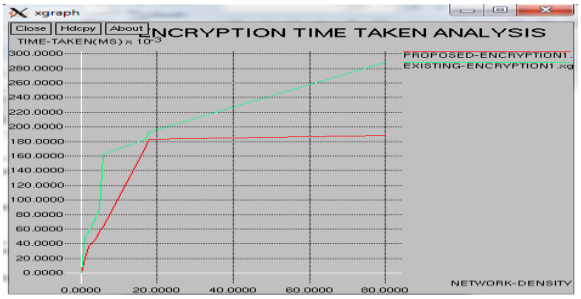

Figure 3(b): Encryption analysis

Encryption time taken in proposed scheme is less compared to existing scheme. Decryption time taken in proposed scheme is less compared to existing scheme

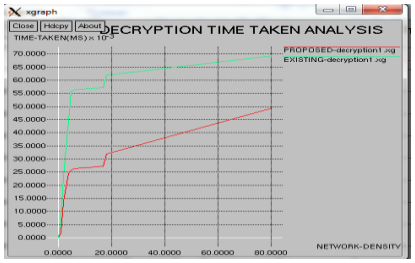

Figure 3(c): Decryption analysis

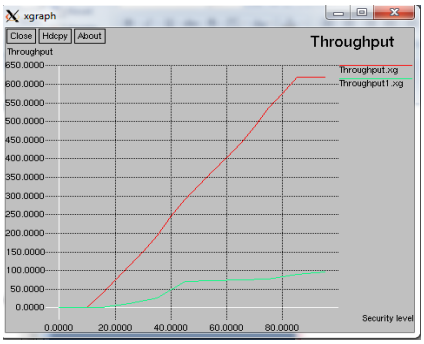

Figure 3(d): Throughput analysis

As security level increases throughput increases

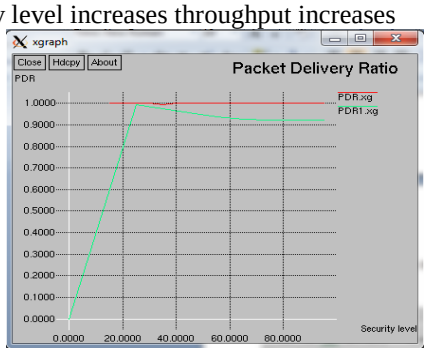

Figure 3(e) : packet delivery Ratio

Packet delivery ratio is constant as security level increases.

8. Conclusion

A source anonymous message authentication scheme (SAMA) based on modified elliptic curve digital signature scheme is proposed here. This scheme provides authenticity. The accelerate signature verification reduces time consuming. This method is simple and requires little additional source. The main advantage is that computational overhead is reduced

References

[1] M. Albrecht, C. Gentry, S . Halevi, and J. Katz, "Attack Cryptographic Schemes Based on 'Perturbation Polynomials', Report 2009/098, http://eprint.iacr.org/, 2009.

[2] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing Symmetric-Key and Public-Key Based Security Schemes in Sensor Networks: A Case Study of User Access Control," Proc. IEEE 28th Int'l Conf. \ Distributed Computing Systems (ICDCS), pp. 11- 18, 2008

[3] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

[4] F. Ye, H. Lou, S. Lu, and L. Zhang, "Statistical En-Route Filtering of Injected False Data in Sensor Networks," Proc. IEEE INFOCOM,Mar. 2004

[5] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004..

[6] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc.IEEE Symp. Security and Privacy May 2000.

[7] D. Point cheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT),pp. 387- 398, 1996

[8] C. Blundo , A. De Santis, A. Herzberg, S. Kutten,U.Vaccaro, And M.Yung"Perfectly Secure Key Distribution Dynamic Conferences,"Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr.1992.

[9] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Comm. ACM, vol. 24, no. 2, pp. 84-88, Feb.1981.

[10] T.A. ElGamal, "A Public-Key Cryptosystem and Signature Scheme Based on Discrete Logarithms," IEEE

Author Profile

Devi Radhakrishnan received the B.Tech degree in Electronics and Communication Engineering from M.G University, Kerala at Mount Zion College of Engineering in 2012. And now she is pursuing her M.Tech degree in Communication Engineering under the same university in Mount Zion College of Engineering.