Pre-distributed Key Authentication and Source Privacy in WSN

S.Balaji, S.Sampath Kumar, B.Sivaraj

***Abstract*— Wireless Sensor Network (WSN) consist of large number of sensor node after deployment these sensor nodes can be captured by the attackers to avoid this many authentication scheme has been developed. Our scheme is based on Elliptic Curve Cryptography (ECC) which provides message source privacy and prevents unauthorized person and corrupted packet from being circulated in the network. It saves the precious sensor energy and every forwarder in the routing path should be able to verify the authenticity of the message upon reception.**

***Index Terms*—Authentication, source privacy, ECC, WSN.**

I. INTRODUCTION

Authentication is a kind of acknowledgment from the controlling factor. In private and public computer networks authentication is commonly done through the use of log on password. Authentication [1] is the process of providing ones identity to someone else. Key management and handling of the pieces of secret information is generally referred to as key management. In our scheme the keys for the nodes which are deployed in the sensor network has been stored in the SS .The nodes which take part in the active transmission get the key for transmission from the security server .The SS will never be compromised. The existing method is based threshold based secret sharing i.e. when the number of transmission is lesser then the threshold value [2] the message is transmitted When the number of transmission is larger than the threshold value the message is completely broken this is the disadvantage of the method . Our proposed method is based on Modified ELGamal Signature based Elliptic Curve Cryptography (ECC). Is used for Authentication generation and Source Anonymous message authentication is used authentication verification. Our scheme provides unlimited message transmission without the threshold problem. It is used to prevent adaptive chosen message attacks it saves the precious sensor energy power. Since the keys are pre distributed in the SS delay is less during the data transmission the nodes get their key from the security server. SS will never be compromised. Each node which takes parts in the transmission has to be registered in the SS.

***Manuscript received Oct 15, 2011*.**

***S.Balaji,** Electronics and communication, Pondicherry University Manakula Vinayagar Institute of Technology Puducherry.*

***S.Sampath Kumar** Electronics and communication, Pondicherry University Manakula Vinayagar Institute of Technology*

***B.Sivaraj** Electronics and communication, Pondicherry University Manakula Vinayagar Institute of Technology Pondicherry*

II. SYSTEM MODEL

Wireless Sensor Network (WSN) consists of large number of sensor nodes after deployment the sensor node may be captured and compromised by the attackers. A SS is responsible for storage, generation of security parameter. SS will never be compromised.

III. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography [3][4][5]is used for polynomial function generation which is used for key generation which is then used to encrypt and decrypt the message .ELGamal is used for encrypt and decrypting the message. If we choose any two points in the circle we get two similar opponents key which is not much efficient .If we choose any two points in the ellipse we get different opponent key therefore the security is increased. Equation of ellipse is

$$E = 4A^3 + 27B^2 + K = 0$$

Where A and B are any two point on the ellipse .The polynomial equation of ellipse is used for key generation.

IV. MODIFIED ELGAMAL SIGNATURE SCHEME (MES)

The modified ELGamal signature [6] scheme consist key generation, signature algorithm, verification algorithm

Key generation: It consist of prime key, generator this key is used for encryption and decryption. The key generation equation is

$$y = g^{x}|p|$$

Where x is a public random number. P is the prime number; g is the range of the prime number.

Signature algorithm: It is used for signature generation the signature algorithm the equation is

$$s = rxh(m,r) + k \mid p-1|$$

Where $r = g^{k}$, where h is the one way hash function. Hash is defined as the exponential of the polynomial where k= zp-1 where zp is the range of the prime number.

Key generation and signature algorithm is used in the sender side for encrypting the d ata.

Verification algorithm: It is used to verify whether the sent key and the received key are same if they are same the data is viewed. The sender and receiver can only view the message other intermediate node can only forward the message. The key size depend upon the size of data

$$g^{s} = ry^{rh(m,r)}$$

Thus the sender side encrypts the message and the receiver side decrypts the message.

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

V. SOURCE ANONYMOUS MESSAGE AUTHENTICATION (SAMA)

Source Anonymous Message Authentication consist of the following steps

Key generation: The key is generated along with the data ELGamal is used for key generation [6][7] since the key is generated before the data transmission the delay is less in this scheme . For a data to be transmitted the nodes get their key from the SS. Data + Anonymous message .The key size depend upon the size of data.

Key verification: Public key of the nodes which take part in the active transmission has to be registered in the SS .For every transmission the nodes interrogate with the SS whether the nodes which take part in the active transmission has been registered in the SS.

Sender Ambiguity : The sender Ambiguity is $\frac{1}{n}$ .Where n is the no of nodes in the AS .Ambiguity Set (AS) is the verified set (i.e.) the node which is registered in the SS take part in the active transmission this set of nodes are called as AS. Before a source node starts the data transmission it gets the public key of the nodes from the SS. This set of nodes are called as AS.

Unforgeability: $n \notin$ AS the node which has been registered in the SS has to take part in the transmission other node does not take part in the transmission .Thus the identity of the source nodes is not revealed.

VI. SOURCE ANONYMOUS MESSAGE AUTHENTICATION ON ELLIPTICAL CURVE

Source privacy[8][9] means the identity of the source is revealed only to the destination node containing the private key .Other intermediate node only partial information is revealed therefore source privacy is achieved. The main objective of the project is to achieve max security level this is achieved by the SAMA on the elliptical curve.

$k_t + \sum_{i \neq t} k_i + r_t d_t h_t \mid n \mid$ is the equation of SAMA on elliptical curve .Where t is the number of transmission , where k is the range of the generator , h is the hash function , and d is the data which is transmitted . The disadvantage of the project is since $i \neq t$ extra transmission is required after the transmission of the message.

Thus different opponent key is generated using the ellipse and ellipse cover larger distance if we use full ellipse then the equation of the ellipse is

$r = x_a \mid n \mid$ Where n is the position of the prime key generator.

VII. SOURCE ANONYMOUS MESSAGE AUTHENTICATION VERIFICATION ALGORITHM

The verification algorithm [10] is used to verify the signature of the sender and the destination node are same .All the nodes which take part in the active transmission could not able to verify the message. Only the source node and the destination node which carry the private key can view the message. Other intermediate node can forward the message. .

The verification equation of the SAMA is $sG - rhaQa \bmod n$ .where s is the signature algorithm where $s = rxh(m,r) + k \mid p-1 \mid$, where $r = g$,Qa is the public key which is stored in the SS , where h is the elliptic curve hash function $E = 4A^3 + 27B^2$+K=0 thus the SS will never be compromised

VIII. ADVANTAGE OF THE SYSTEM

The advantage of this scheme is security level is high since two different opponent key

- The time taken for encryption and decryption of the message is less
- In scheme Max number of connection served per unit time is very high
- The Data flow rate is of this scheme is high

These are some of the advantage of this scheme.

IX. SIMULATION RESULT

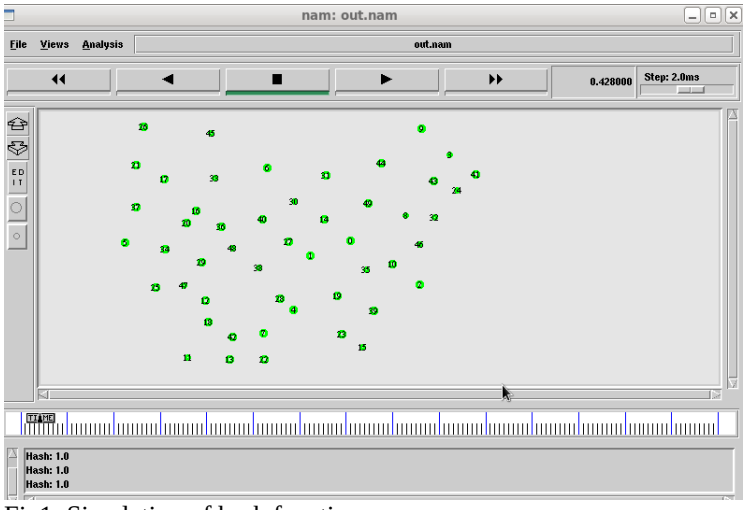

Fig1: Simulation of hash function

The fig illustrates the generation of hash function and the total number of nodes deployed in the network. The nodes which take part in the active transmission have to be registered in the SS. The SS will never be compromised .The total no of nodes deployed in the WSN is 50.

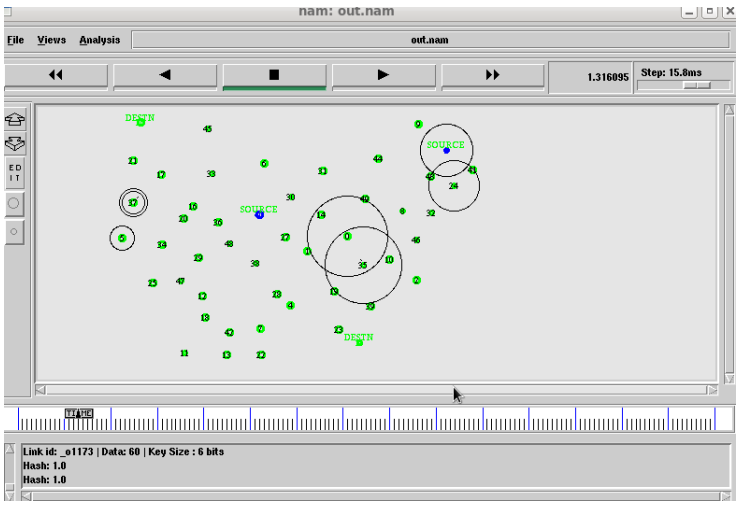

Fig2 : Data transfer

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR

The fig illustrates the data transfer in the WSN. the data is transmitted along with the key by the source node other intermediate nodes in the WSN can only forward the message using the public key which is stored in the SS .All the nodes which take part in the transmission has to be registered in the SS.,

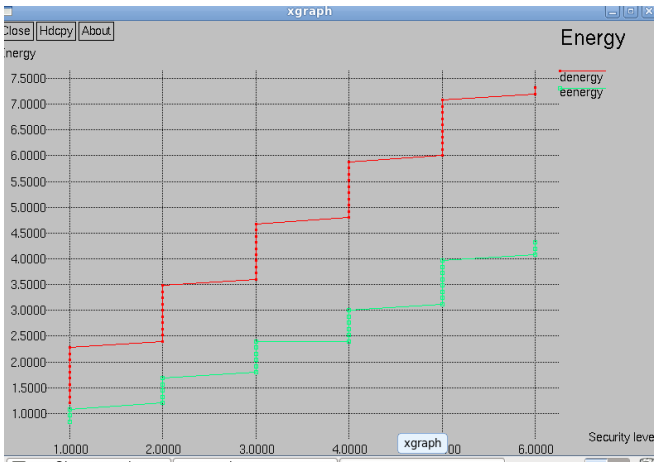

Fig 3 : Energy consumption of ELGamal vs DES

The above fig illustrates the energy consumption of ELGamal vs DES. Since the key size is large in DES the energy consumption of DES is large. Our scheme provides max security with min energy.

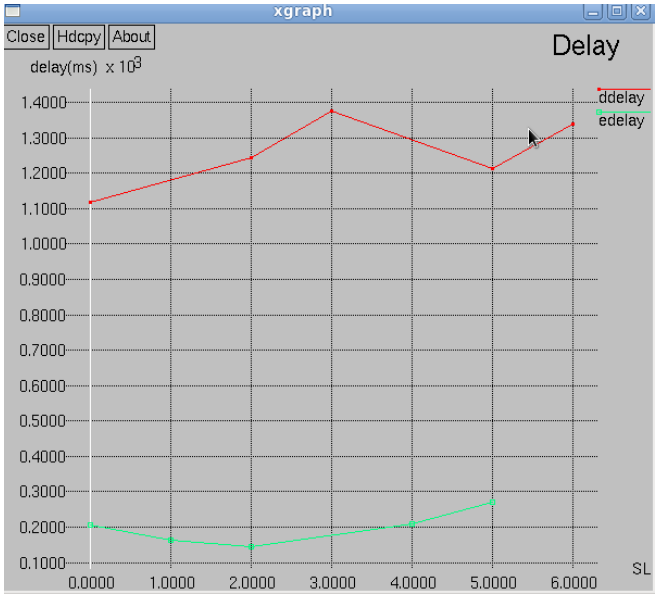

Fig 3 : Delay of ELGamal vs DES

The above fig illustrates the delay of ELGamal vs DES. Since the key size is large in DES the delay consumption of DES is large. Our scheme provides max security with min delay. Since the keys are pre distributed in the SS the delay is less in ELGamal .

X. CONCLUSION

Thus system provides maximum security with minimum energy. Mover over the delay is also less when compared to the other system thus Source Anonymous message authentication on elliptic curve provides maximum security with minimum energy

REFERENCES

[1] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless Sensor Network Security: A Survey," *Auerbach Publications*, CRC Press,2006

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

[3] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors, *Advances in Elliptic Curve Cryptography*, London Mathematical Society Lecture Note Series 317, Cambridge University Press, 2005.

[4] Hankerson, D.; Vanstone, S.; Menezes, A. (2004).*Guide to Elliptic Curve Cryptography*. Springer Professional Computing. New York: Springer. doi:10.1007/b97644. ISBN 0-387-95273-X

[5] Certicom Research, Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 2.0, May 21, 2009.

[6] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology CRYPTO 92, LNCS 740, pages 471486, 1993.

[7] R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, pp. 120- 126, 1978

[8] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/pdf, Feb. 2008

[9] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transaction,"ACM Trans. Information and System Security, vol. 1, no. 1, pp. 66-92, 1998

[10] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000

S.BALAJI M.Tech student of Electronics and Communication Engineering in Manakula Vnayagar Institute of Technology affiliated to Pondicherry University

S.SAMPATH KUMAR Associate Professor of Electronics and Communication Engineering in Manakula Vnayagar Institute of Technology affiliated to Pondicherry University

B.SIVARAJ M.Tech student of Electronics and Communication Engineering in Manakula Vnayagar Institute of Technology affiliated to Pondicherry University

ISSN: 2278 – 7798 All Rights Reserved © 2015 IJSETR