ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Source Anonymous Message Authentication (SAMA) In WSN : A Review

Vandna[1]

M.Tech Student, Department of Computer science & Engineering, University Institute of Engineering & Technology, M.D. University, Rohtak, Haryana, India[1].

ABSTRACT: Message authentication is one of the most effective ways to abduct unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs).Many ordinary methods have been developed, they are symmetric key and public key cryptosystem. But they have their own limitations of high computational overhead, communicational overhead and deficiency of scalability. To reduce these problems a polynomial based scheme was developed but they have the limitations with the threshold value i.e ,the number of messages transmitted should be less than the threshold value.In this paper,we consider a source anonymous message authentication scheme(SAMA) based on elliptic curve cryptography which permit intermediate authentication. By this scheme any node can transmit an unlimited number of messages without threshold problem and also gives message source privacy.

KEYWORDS:SAMA, Polynomial, ElGamal, WSN, ECC**.**

I. INTRODUCTION

Message authentication plays a key role in avert unauthorized and corrupted messages from being forwarded in WSN to save the precious sensor energy [1]. Message authentication scheme is divided into two categories they are symmetric-key based approaches and public key based approaches. The symmetric-key based approach needs complicated key management and having scalability problem and is not resilient to node compromise attacks and same key is shared between sender and receiver. By abduct a single node an intruder can easily compromise the key and it does not work in multicast networks.

The public-key based approach, each message is transmitted along with the digital signature of the message generated using the sender's private key. Each intermediate forwarder and final receiver can perform the authentication of the message using sender's public key. The recent progress on elliptic curve cryptography (ECC) shows that the public key schemes can be more useful in terms of computational complexity, memory usage, and security resilience and it also having a simple and clean key management. In this paper, we discuss a secure and ell organise source anonymous message authentication(SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. SAMA every intermediate node can authenticate the message so that all the unauthorized and corrupted messages can be found out and dropped to conserve the sensor power. This scheme does not have any threshold problem; any node can transmit an unlimited number of messages.

II. LITERATURE REVIEW

An unconditional secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified ElGamal signature (MES) scheme on elliptic curves. This scheme enables the intermediate nodes to authenticate the message so that does not have threshold problem. Efficient key management framework to ensure isolation of the compromised nodes.Offer an efficient source anonymous message authentication mechanism for WSNs without the threshold limitation. While achieving compromise- resiliency, flexible-time authentication and source identity protection, our scheme does not have the threshold problem. SAMA is more efficient than the polynomial-based algorithms under comparable security levels. a source anonymous message authentication (SAMA) on elliptic curves that can provide unconditional source anonymity. The recent progress on elliptic curve cryptography (ECC)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

shows that the public-key schemes can be more advantageous in terms of memory usage, message complexity, and security resilience since public-key-based approaches have simple and clean key management

Naipuniya HC et al [5] Introduce Polynomial-based technique for terminate of computational overhead, increasing the scalability, fastening the authentication and exchange of unlimited number of messages. It shows computation and communication overhead and also gives high level of security and source privacy. In this scheme packets are sent first and then the message, digital signature is advanced and can be accessed by legitimate sender and receiver. To reduce delay time and scalability is increased, no threshold is observed, unlimited packets can be transmitted and message reaches the destination without any attacks.

W. Zhang et al [6] Introduced A secret polynomial-based message authentication scheme which gives information theoretic security with ideas similar to a threshold secret sharing scheme, where the threshold is decided by the degree of the polynomial. When the number of messages transmitted is below the threshold, the scheme enables the intermediate node to verify the authenticity of the message through polynomial evaluation.

M. Albrecht et al [7]Proposed hop by hop message authentication without the weakness of the form in threshold of the polynomial based scheme. SAMA based on ECC compared it against other popular mechanisms in different scenarios through simulations and TelosB.Results indicate that it greatly increases the effort of an attacker, but it requires proper models for every application. Proposed scheme is more systematic than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

Mohamed-LamineMessai [8] Introduce message sender anonymity based on ring signature. This approach able the message sender to generate a source-anonymous message signature with content authenticity assurance. ring signature used in all the applications ,different kinds of security algorithms like symmetric key algorithm and public key algorithm.

Tarun Narayan [9] Introduce brief overview of elliptic curve cryptography and have developed an alphabetical table for ECC data encryption and decryption in a better manner. The strength of encryption depends on its key and if we use the alphabetical table then Runtime will be faster by this process, uses of alphabetical table will gives better performance in this regard. Public key is used for message encryption in the case of socket layer security.

Mangesh M. Ghonge and Minal S. [10] Introduce a polynomial-based scheme this scheme and its supplement all have the weakness of a built-in threshold determined by the degree of the polynomial: result shows When SAMA can be applied to any messages to provide hop-by-hop message placid authenticity select shortest path without the weakness of the built-in threshold of the polynomial-based scheme.

III. SAMA DESIGN GOALS

1. Message authentication: Each message receiver should be able to verify whether a received message is Sent by the node that is declared. The rival cannot act as an innocent node.
2. Message integrity: Each message receiver should be able to verify whether the message has been Modified the rival.
3. Hop-by-hop message authentication: Every intermediate node along the routing path should be capable to verify the authenticity and integrity of the message.
4. Identity and location privacy: By analyzing message content, the rival cannot check the message ID and location.
5. Node compromise resilience: It should be resilient to node compromise attacks.
6. Efficiency: The SAMA scheme is efficient in terms of both computational and communication overhead.

IV. TECHNIQUES IN ENCRYPTION

Symmetric key encryptionin symmetric key encryption there is a secrete key its uses for same secrete key to encrypt or decrypt the data .Secrete key be known by the partial encryption the data and partially decryption data. Both time it uses the same key.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

Public key encryption any person can encrypt a message using the public key of the receiver, but these message can be decrypted only with the receiver's private key. For this to work it must be computationally easy for a user to generate a public and private key-pair to be used for encryption and decryption. Two keys uses for encryption and decryption.
Elliptic curve cryptography (**ECC**) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC require smaller keys compared to non-ECC cryptography to provide equivalent security. ECC is easy than the non ECC cryptography.
These do not require any shared key.
The mathematical operation of ECC is a = b+rb+s
Where r +s ≠ 0
Change in r and s value gives different elliptic curve. All points (a, b) and a point at infinity on the elliptic curve will satisfice the above equation.

EIGamal signature scheme (**ESC**) EIGamal signature scheme will get implemented to verify the sent message or the data packet to save the energy of each intermediate node between source and its respective destination.
The MES scheme consists of the following three algorithms:

1. Key generation algorithm: Let p be a enormous prime and g be a generator: Both p and g are make public. For aunsymmetrical private key x, the public key y is computed from y = gx mod p.

2. Signature algorithm: The MES can also have many alternatives. For the justification of efficiency, we will describe the alternative, called optimal scheme. To sign a message m, one select a random k , then computes the exponentiation r = gk mod p and solves s from:
s = rxh (m, r) +k mod (p-1),
where h is a one-way hash function.
Signature of message m is defined as the pair(r, s).

3. Verification algorithm: The verifier check whether the signature equation gs =ryrh (m, r) mod p: If the Emancipation holds true, then the evidence accepts the signature, and otherwise reject.

V. SOURCE ANNOYMOUS MESSAGE AUTHENTICATION

There will be many sensor nodes in wireless sensor network. Locations of these nodes are monitored with the help of specialized transducers. SAMA is public key crypto system key generation is based on elliptic curve cryptography. Each intermediate node transmit the message with authenticate the message. To check whether the message is modified or not. SAMA allowstransmit unlimited number of message. It also has very less threshold problem. A source anonymous message authentication is based on MES scheme on elliptic curve.
SAMA consists of mainly two algorithms:

1. Generate (m, Q1 ,Q2,..., Qn): Given a message m and the public keys Q1,Q2,..., Qn of the AS (ambiguity set) S = { A1 , A2,...,An}, the actual message sender At,1 ≤ t ≤ n, produce an anonymous message S(m) using its own private key dt.
2. Verify S(m): Given a message m and an anonymous message S(m), which includes the public keys of all members in the AS, a verifier can determine whether S(m) is generated by a member in the AS.

Technique	Drawback
SEF(statistical En-route Filtering)	SEF does not address the issues of how to recognize the compromised nodes.
ECC-based access control	Scalability is less. Less Efficiency.
Polynomial-based technique	High Congestion. Less Efficient.

Table1. Comparison ofExisting Technique& Drawback

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor & UGC Approved Journal)

Website: www.ijirset.com

Vol. 6, Issue 9, September 2017

VI. CONCLUSION

The message authentication is used to avert the unauthorized and lawless message being forwarded in the WSN. A novel and logical SAMA based on ECC can be applied to any message to give message content authenticity. It gives hop-by-hop message authentication without the debility of built in threshold of the polynomial based scheme. SAMA scheme not only a efficiency in authentication but also gives extra source privacy.

REFERENCES

[1] S.S. Manavi, M.S. Kakkasageri, D.G.Adiga, "Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach,"IEEE in ICFCC, 2009.120,(2009).

[2] L. Harn and Y. Xu, "Design of generalized ElGamal type digital signature Schemes based on discreet logarithm," Electronics Letters, vol. 30, no. 24, pp. 2025–2026, (1994).

[3] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in Advances in Cryptology - Crypto'92, Lecture Notes in Computer Science Volume 740, pp. 471–486, (1992).

[4] N.Gura, A.Patel, A.W, H.Eberle, and S.C.Shantz, "Comparing elliptic curve cryptography and rsa on 8- bit cpus," pp. 1 19-132,(2004).

[5] Naipunya HC, Nalina GR, Gururaj H L, Ramesh B "Secured Source Anonymous Message Authentication Using Wireless Sensor Network" IOSR Journal of Computer Engineering, Volume 17, Issue 3, Ver. III, PP.17-20 (May – Jun. 2015).

[6] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise resilient message authentication in sensor networks," in IEEE INFOCOM, (Phoenix, AZ.), (April 15-17 2008).

[7] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials" Cryptology ePrint Archive, Report 2009/098, (2009).

[8] Mohamed-LamineMessai, "Classification of Attacks in Wireless Sensor Networks",International Congress on Telecommunication and Application'14 University of A.MIRA Bejaia, Algeria,pp- 23-24 (APRIL 2016).

[9] Tarun Narayan Shankar, "Cryptography With Elliptic Curve,"International Journal Of Computer Science And Applications, Vol. 2,(April / May 2009).

[10] Mangesh M. Ghonge, Minal S. "Implementation of Message Authentication Scheme for Elliptic Curve Cryptography in Wireless Sensor Networks", 4099 Themed Section: Engineering and Technology, volume 2, PP-322-326 (March 2016).

[11] S.Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks,"Third IEEE International Conference on Pervasive Computing and Communications, (Washington, DC, USA), pp. 324-328, (2005).

[12] N. Gura, A. Patel, A. W, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," pp. 1 19-132, 2004.