IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. III (May – Jun. 2015), PP 17-20
www.iosrjournals.org

Secured Source Anonymous Message Authentication Using Wireless Sensor Network

[1]Naipunya H C, [2]Nalina G R, [3]Gururaj H L, [4]Ramesh B
[1,2]*Department of Computer Science & Engineering, Malnad College of Engineering, Hassan*
[3]*Assistant Professor, Department of CS&E, Malnad College of Engineering, Hassan, India*
[4]*Head of Department, Department of CS&E, Malnad College of Engineering, Hassan*

***Abstract*:** *The secured exchange of message was the main concern. To overcome this, message authentication schemes were developed, to maintain the privacy of message. Message authentication schemes are based on symmetric key or public key cryptosystem. This resulted in lack of scalability, delayed authentication, communication overhead, high computation, etc. To address these issues we propose a new system called Secured Authentication and Source Privacy (SASP) for Message based on Elliptic curve cryptography (ECC). This scheme adopts Polynomial-based technique for the elimination of computational overhead, increasing the scalability, fastening the authentication and exchange of unlimited number of messages. This analysis and simulation depending on our proposed system is far more efficient than previously existing Source Anonymous Message Authentication (SAMA) in terms of computation and communication overhead and also provides high level of security and source privacy.*

***Keywords*:** *Signature, Authentication, Elliptic Curve Cryptography (ECC)*

I. Introduction

When a wireless sensor network is implemented in rough environment, the opponent may collect and alter sensor node, or insert their sensor node to the network and provoke the network to accept these new nodes as legitimate nodes. The most common attack is message authenticity and integrity. For example, if the sender and receiver are in the different transmission range, a third party on the path connecting them can alter the message or insert a new inappropriate message. A solution for this problem is to share a secret key and shared key between sender and receiver using message authentication code (MAC). This however does not provide authentication because a compromised receiver can fake a MAC [1]. To overcome this, digital signatures were used. Each message is transmitted along with the digital signature generated using a sender private key. Modified Elgamal Signature (MES) scheme is based on difficulty of computing discrete logarithms [3][4]. This allows a third party to authenticate a message in a insecure channel. For a ring signature, elliptic curves based on MES scheme are generated[4]. Each member generates a ring signature and this is computed as forgery signature for all other members in the ambiguity set. Ambiguity set minimizes the probability of error occurrence during message authentication[5]. Every intermediate forwarder node and final receiver node will authenticate the message using sender public key. The proposed SASP aims to reduce congestion and privacy related issues and introduced more reliability in wireless transmission range. This should satisfy entity authentication, message non-repudiation, access control reliability identification, privacy and anonymity [2].

II. Related Work

For SASP of message we use public cryptosystem. The previously generated SAMA is verified in a more reliable equation without individually. The SAMA generation is based on MES scheme of elliptic curve. Each message 'x' to be sent, the message sender, or the sending node generates secured authentication and source privacy of message x.

A. Modified Elgamal Signature (MES)

A signature scheme cannot be completely secure. This is based on discrete logarithms. This scheme allows the authentication of a message sent by a third party to conform over an insecure channel.

- Randomly choose a secrete key s with $1<s<p-1$.
- Compute $r=m^s \bmod p$.
- Public key is (p, m, r).
- The secrete key is s.
- These steps are to be performed by signer.
- Choose a random t such that $1<t<p-1$ and $\gcd(t,p-1) =1$
- Compute $a=m^t \pmod p$.

- Compute $z= (H(x)-sr)t^{-1} \pmod{p-1}$.
- If z=0 start over again.

A third party can forge signature either by finding signer secrete key s or by finding hash function.
$H(x) \equiv H(X) \pmod{p-1}$ signer must carefully choose t uniformly at random for each signature. If multiple messages are using same key an attacks can directly computes [3][6].

B. Source Anonymous Message Authentication (SAMA)

There will be numerous sensor nodes in wireless sensor network. Locations of these nodes are monitored wish the help of specialized transducers. SAMA is public key crypto system key generation is based on elliptic curves.

Each intermediate node transmitting the message will authenticate the message. To check if the message is modified or not. SAMA allows unlimited number of transmission. It also has very less threshold problem. A source anonymous message authentication is based on MES scheme on elliptic curve.
The generation of SAMA is based on MES algorithm.

C. Elliptic Curve Cryptography (ECC)

ECC is public key cryptography. Uses taking part in communication will have a pair of public key and private key and operations linked with three keys. Some public key predefine domain parameters [2] in ECC. These do not require any shared key.
The mathematical operation of ECC is $a^2 = b^3+rb+s$
Where $4r^3+27s^2 \neq 0$
Change in 'r' and 's' value gives different elliptic curve. All points (a, b) and a point at infinity on the elliptic curve will satisfy the above equation.
Public key is a point on the curve and private key is a random number. Public is the product of private key and a generator point P. ECC uses very small key size. A 160-bit is equal to 1024-bit of RSA algorithm.

III. Proposed Methodology

We propose an advanced method of source privacy and message authentication , SASP. The implication of this method gives considerably a high rate of advancement in securing the message. Accurate verification is made both at the sender and receiver end.

A. SASP of message, on a Elliptic Curve based on MES of SAMA

According to MES, Receiver verification and sender verification must be equal. If it's not equal, then it confirms the impeding of the message.
Let P=large prime number.
i=private integer ($1 \leq i \leq P-2$).
$\beta=\alpha^i \pmod{P}$
Public: P, α, β.
α =primitive root
Sender= (x, a, b) and n is random private number.
$P= \alpha^n \bmod p$
$S= n^{-1} (x-ia) \pmod{p-1}$
S=secret key

Verification:
For sender:
$V1= [\beta\, a^b \pmod{p}]*i$
For receiver:
$V2=[\alpha^x \pmod{p}]*i$
If V1=V2, signature is valid else signature is not valid [1][2][3][6].

Multiplying 'i' (private key) at the verification step increases the security. As i is a secrete key, only a sender and an authenticated receiver will be able to access this key.

When multiplied, both sender and receiver's verification value should be same else authentication is encumbered.

This gives increased correctness and high communication quality. Third party attack is reduced, through the intermediate nodes the message is transmitted to the destination node, these intermediate nodes cannot access the message.

IV. Comparative Analysis Of Delay In MES, SAMA and SASP

Broad comparision between MES , SAMA and SASP in XY-graph is done in this chapter. It provides a better understanding of working and efficiency of SASP.

A. End to End Delay

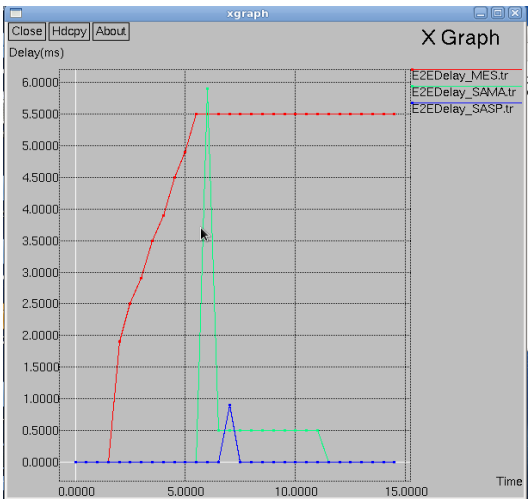

Figure 4.1 End to End Delay

It is observed that MES takes more time to send the message. The delay time and range in MES is high as depicted in Figure 4.1

In SAMA, delay range is low compare to MES and the message is sent in a short time and delivered to the destination at the earliest.

SAMA-SASP in the above graph we observe, SASP sends the message faster than SAMA, in a secure channel without any delay. This reduced communication time, exchange of message between sender and receiver is fast end.

B. Packet Delivery Ratio

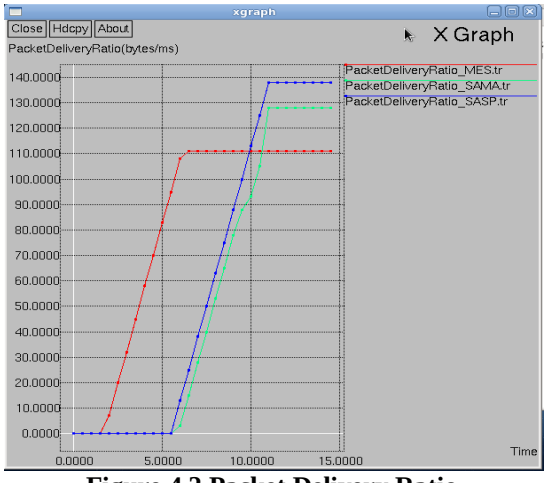

Figure 4.2 Packet Delivery Ratio

MES-SAMA: SAMA has higher delivery ratio than MES. SAMA decrease the time taken to deliver a message. When compared to MES scheme. Message is delivery quickly without altering the message number, third party can access the message depicted in Figure 4.2

SAMA-SASP, the delivery ratio of SAMA is considerably low. SASP acts faster than SAMA and is more efficient carrier of the message.

C. Packet Loss Ratio

With the implementation of these improved newer algorithm. We can achieve 0 packet loss depicted in Figure 4.3. Message can be transmitted through nodes without any loss of packet. Packets are exchanges first and then message is exchanged without the range generated. This increase the efficiency and security of the signature.

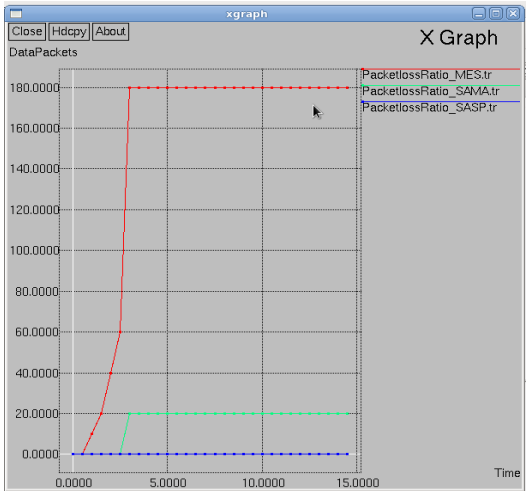

Figure 4.3 Packet Loss Ratio

V. Conclusion

The primary aim in wireless sensor networks is to increase the security, authenticity and privacy. The basic principle of encryption, decryption, key exchange, verification and working of the algorithms are explained, to support our proposed polynomial based technique to achieve these goals. Here packets are sent first and then the message, digital signature are advanced and can be accessed by legitimate sender and receiver. Reduces delay time and scalability is increased, no threshold is observed, unlimited packets can be sent and message reaches the destination without any attacks.

References

[1]. W. Zhang, N. Subramanian, and G. ang, "Lightweight and compromise resilient message authentication in sensor networks," in IEEE INFOCOM, (Phoenix, AZ.), April 15-17 2008.
[2]. S.S. Manavi, M.S. Kakkasageri, D.G.Adiga, "Message Authentication in Vehicular Ad hoc Networks: ECDSA Based Approach," in ICFCC, 2009.120, 2009 IEEE.
[3]. Mojtaba Gorbanaliadeh, Mahmood Javadi, Kiomars Abdi, Ali Hosseinalipour, "Error detection in wireless sensor networks based on Assertion functions," Volume 4, Issue 5, May 2014 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineerinng.
[4]. Yun Li, Jie Wu, Jian Li, Jian Ren, "Providing Hop-by-Hop Authentication and Source Privacy in Wireless Sensor Networks,"2012 IEEE.
[5]. D. Pointcheval and J. Stern, "Security proofs for signature schemes," In Advances in Cryptology - EUROCRYPT, Lecture Notes in Computer Science Volume 1070, pp. 387–398, 1996
[6]. 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
[7]. 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
[8]. User access control," in IEEE ICDCS, (Beijing, China), pp. 11–18, 2008
[9]. R. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in Advances in Cryptology–ASIACRYPT, Lecture Notes in Computer Science, vol2248/2001, Springer Berlin / Heidelberg, 2001.