Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.155 – 160

RESEARCH ARTICLE

Source Anonymous Message Authentication Based On ECC in Wireless Sensor Networks

B.Renugadevi[1], T.John Peter[2]

[1]PG Scholar, Department of Computer Science and Engineering, Anna University Chennai, India

[2]Assistant Professor, Department of Computer Science and Engineering, Anna University Chennai, India

[1, 2] Roever Engineering College, Perambalur

[1] renugacse12@gmail.com, [2] johnthiraviam85@gmail.com

Abstract—Source Anonymous Message authentication (SAMA) is one of the most effective ways to prevent unauthorized and corrupted messages from being forwarded in wireless sensor networks (WSNs).A scalable authentication scheme based on elliptic curve cryptography (ECC) is introduced to allow any node to transmit an unlimited number of messages without suffering the threshold problem and provides message source privacy. For each message the sending node generates a source anonymous message authenticator for the message. The generation is based on MES scheme on elliptic curves. An efficient key management framework is introduced to ensure isolation of the compromised nodes. ECC reduces computational and communication overhead under comparable security levels while providing message source privacy.

Keywords— Hop-by-hop authentication; symmetric key cryptosystem; public-key cryptosystem; source privacy; Modified Elgamal Signature (MES)

I. INTRODUCTION

The Wireless Sensor Network consists of a large number of sensor nodes. Each sensor node knows its relative location in the sensor domain and is capable of communicating with its neighbouring nodes directly using geographic routing. Message authentication plays a vital role in preventing corrupted message from being forwarded in network to save precious sensor energy. Message authentication schemes can be divided into two categories public key based approach and symmetric key based approaches.

The symmetric key based approach requires complex key management is not resilient to node compromise attacks since both sender and receiver have to share a secret key. By capturing a single sensor node an intruder can compromise the key. Multicast network does not work in symmetric key based approach.

To solve the scalability problem, a secret polynomial based message authentication scheme was introduced. The idea is similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. The intermediate nodes verify the authenticity of the message through a polynomial evaluation. When the number of messages transmitted is larger than the threshold, adversaries fully recovered and the system is completely broken.

Each message is transmitted along with the digital signature of the message generated using the sender's private key in public key based approach. One of the limitations is the high computational overhead. The recent progress on elliptic curve cryptography (ECC) shows that this can be more advantageous in usage of memory, and resilience security.

An unconditionally secure and efficient source anonymous message authentication (SAMA) scheme based on the optimal modified Elgamal signature (MES) scheme on elliptic curves is introduced. This MES scheme is secure against adaptive chosen-message attacks in the random oracle model.

The major contribution is first to develop a source anonymous message authentication on elliptic curves that can provide an unconditional source anonymity. Secondly, offering efficient hop by hop message authentication for WSN without threshold limitation. Thirdly, an efficient key management framework is introduced to ensure isolation of compromised nodes.

II. RELATED WORK

Message authentication are used in different applications and security is one of the key characteristic of all the applications for that, many authors proposed different kinds of security algorithms like symmetric key algorithm and public key algorithm. Both passive and active attacks are discussed in that algorithms and also recovery mechanisms are shown in simulation. The advantages and disadvantages of such algorithms are discussed below.

A .STATISTICAL ENROUTE FILTERING

Statistical En-route Filtering (SEF) mechanism detects and drops false reports. SEF requires each sensing report must be validated by multiple keyed message authentication codes (MACs), each generated message by a node that detects the same event. As the report is forwarded, each node verifies the correctness of the MACs probabilistically and drops those invalid MACs at earliest points. The sink filters out remaining false reports that escape the enroute filtering. SEF exploits to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding.

The limitation it fails to detect malicious misbehaviours with the presence of the following disadvantages like ambiguous collisions, receiver collisions, limited transmission power, false misbehaviour report, collision and partial dropping.

B.SECRET POLYNOMIAL MESSAGE AUTHENTICATION

A secret polynomial based message authentication scheme was introduced to prevent message form adversaries. This scheme offers security with ideas similar to a threshold secret sharing, where the threshold is determined by the degree of the polynomial. If the number of messages transmitted is below the threshold, then the intermediate node to verify the authenticity of the message through polynomial evaluation. When the number of messages transmitted is larger than the threshold, the polynomial be fully recovered by adversary and the system is broken completely. To increase the threshold for the intruder to reconstruct the secret polynomial, a random noise, also called a perturbation factor, was added to the polynomial to prevent the adversary from computing the coefficient of the polynomial.

III. PROPOSED WORK

A. SYSTEM MODEL

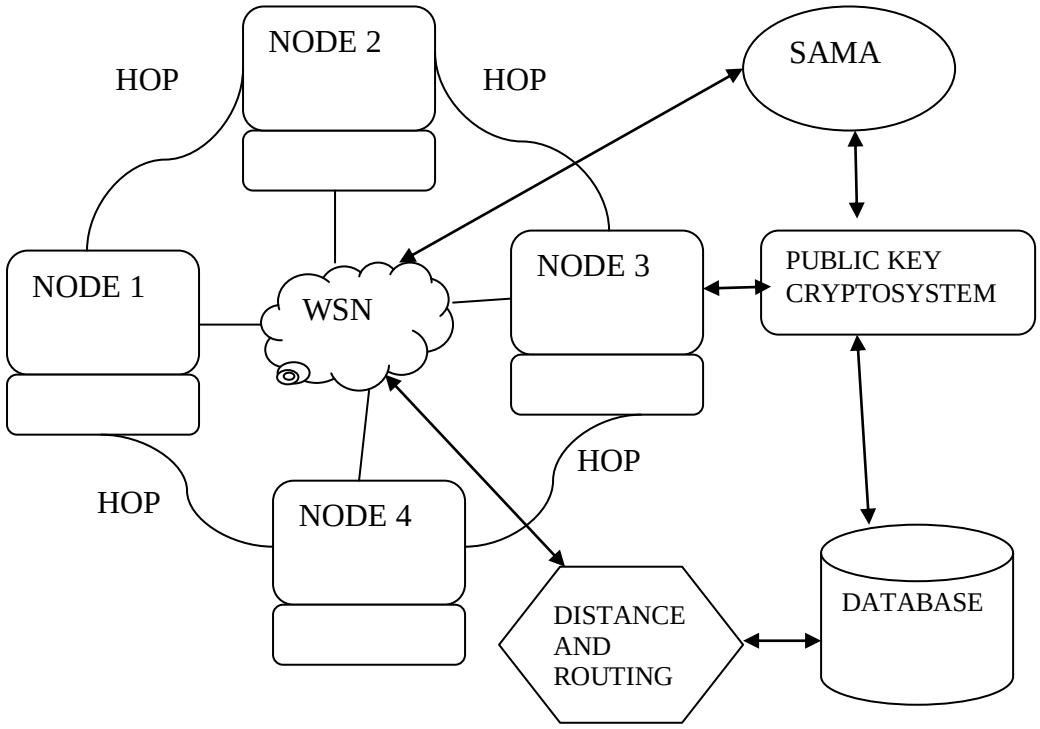

Fig.3.1. System Architecture

This is the improved form of SAMA it generates a source anonymous message authenticator for the message. The generation is based on MES scheme on elliptic curves. SAMA generation requires three steps, which link all non-senders and the message sender to the SAMA. SAMA is verified through a single equation without individually verifying the signatures.

B. MES SCHEME ON ELLIPTIC CURVES

Let $p > 3$ is an odd prime. An elliptic curve E is defined by an equation of the form:

$$E: \; y^2 = x^3 + ax + b \bmod p,$$

SIGNATURE GENERATION ALGORITHM:

The signer performs the following steps to sign a message m.

1. Choose a random k such that $0<k<p-1$ and gcd (k, p-1)=1.
2. Compute $r \equiv g^k \pmod p$.
3. Compute $S \equiv (H(m)-xr)\, k^{-1} \pmod{p-1}$.
4. If s=0 start over again.

Then the digital signature of m is the pair(r, s).
For every signature the signer repeats these steps.

VERIFICATION ALGORITHM:

A signature (r,s) of a message m is verified as follows.

1. $0<r<p$ and $0<s<p-1$.
2. $g^{H(m)} \equiv y^r r^s \pmod p$.

CORRECTNESS:

The algorithm is correct only a signature generated with the signing algorithm will always be accepted by the verifier.

The signature generation implies

$$H(m) \equiv xr + sk \pmod{p-1}.$$

Hence Fermat's little theorem implies

$$\begin{aligned} g^{H(m)} &\equiv g^{xr} g^{ks} \\ &\equiv (g^x)^r (g^k)^s \\ &\equiv (y)^r (r)^s \pmod p. \end{aligned}$$

C. COMPROMISED NODE DETECTION

When a node has been identified as compromised, the SS can remove its public key from its public key list. It can also broadcast the node's short identity to the entire sensor domain so that any sensor node that uses the stored public key for an AS selection can update its key list. Once node compromised is detected it should be dropped in order to save the precious sensor power.

IV.PERFORMANCE EVALUATION

A. Simulation model and parameters

To evaluate the performance of proposed system, compare it with some existing techniques using NS-2 Simulator. The bivariate polynomial based scheme is a symmetric key based implementation, while proposed scheme is based on ECC. Assume that the key size to be *l* for symmetric key cryptosystem, the key size for proposed should be *2l* which is much shorter than the traditional public key cryptosystem. The

simulation parameters are helpful in simulating the proposed system. Table 1 shows the process time for existing scheme and Table 2 shows the process time for proposed scheme.

TABLE 1
PROCESS TIME FOR EXISTING SCHEME

	Polynomial based approach			
	dx,dy=80		dx,dy=100	
	Gen	Verify	Gen	Verify
L=24	9.31	0.25	14.45	0.31
L=32	12.95	0.33	20.05	0.41
L=40	13.32	0.35	20.57	0.44
L=64	21.75	0.57	33.64	0.71

TABLE 2
PROCESS TIME FOR PROPOSED SCHEME

	Proposed approach			
	n=1		n=10	
	Gen	Verify	Gen	Verify
L=24	0.24	0.53	4.24	2.39
L=32	0.34	0.80	5.99	3.32
L=40	0.46	1.05	8.03	4.44
L=64	1.18	1.77	20.53	11.03

B. Performance Metrics

The ECC scheme is compared against polynomial based and it has provided the positive results.

Packet delivery ratio (PDR): PDR defines the ratio of the number of packets received by the destination node to the number of packets sent by the source node.

Routing overhead (RO): RO defines the ratio of the amount of routing-related transmissions [Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR), ACK, S-ACK, and MRA].

Delay: Delay is the interarrival time of 1st and 2nd packet to that of total data packets delivered.

C. Results

Enhanced message authentication scheme is evaluated by comparing it with other existing algorithms using the NS-2 Simulator. Fig 4.1 shows Packet Delivery Ratio of the proposed method over other existing methods.

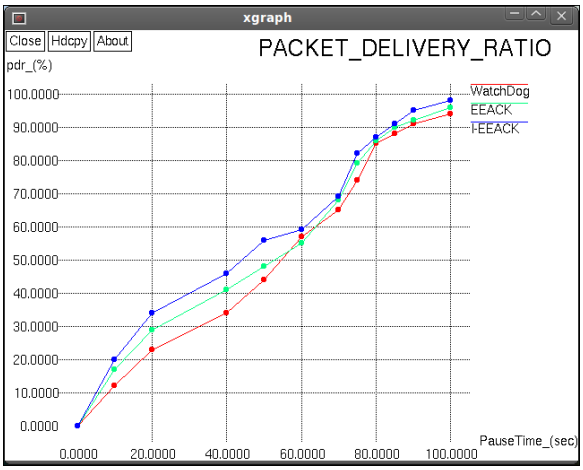

Figure 4.1 Packet Delivery Ratio

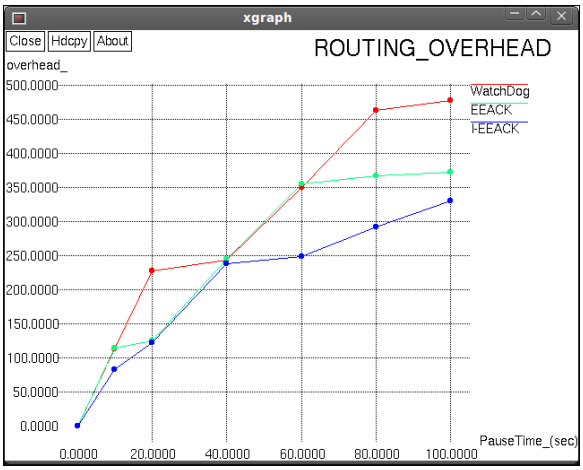

Figure 4.2 Network Overhead

V. CONCLUSION

Message authentication has always been a major threat to the security in wireless sensor Networks. A Novel and efficient source anonymous message authentication scheme based on ECC to provide message content authenticity. To provide hop by hop message authentication without the weakness of the built in threshold of the polynomial based scheme. SAMA based on ECC compared it against other popular mechanisms in different scenarios through simulations and TelosB.

Simulations results indicate that it greatly increases the effort of an attacker, but it requires proper models for every application. Proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

ACKNOWLEDGMENT

I would like to thank Mr.T.John Peter Assistant Professor in Roever Engineering College, Perambalur for guiding me to bring this paper successful.

REFERENCES

[1] F. Ye, H. Lou, S. Lu, and L. Zhang, "*Statistical en-route filtering of injected false data in sensor networks*," in IEEE INFOCOM, March 2004.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "*An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks*," in *IEEE* Symposium on Security and Privacy, 2004.

[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, ser. Lecture Notes in Computer Science Volume 740, 1992, pp. 471–486.

[4] 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.

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

[6] D. Pointcheval and J. Stern, "*Security proofs for signature schemes*," in Advances in Cryptology - EUROCRYPT, ser. Lecture Notes in Computer Science Volume 1070, 1996, pp. 387–398.

[7] D. Pointcheval and J. Stern, "*Security arguments for digital signatures and blind signatures*," Journal of Cryptology, vol. 13, no. 3, pp. 361–396, 2000.

[8] 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*," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[9] A. Perrig, R. Canetti, J. Tygar, and D. Song, "*Efficient authentication and signing of multicast streams over lossy channels,"* in IEEE Symposium on Security and Privacy, May 2000.

