Available at: www.researchpublications.org

Analysis of Privacy in WSN's by providing Hop-by-Hop Message Authentication

Roshni R. Kharche[1], Lokesh Bijole[2]

[1] *Post Graduate Student, Department of CE, Padm. Dr. V.B.K.C.O.E., Malkapur, S.G.B.A. University, Maharashtra, India*

[2] *Asst. professor, Department of CSE, Padm. Dr. V.B.K.C.O.E., Malkapur, S.G.B.A. University, Maharashtra, India*

[1]*roshnikharche.cse@gmail.com*

[2]*lokeshmits5588@gmail.com*

***Abstract*—Confidentiality and security to the data is actually provided by an authentication technique. Itgives the confident identification of one party by another party or a process of confirming an identity .But now, there are various methods for authentication such as Signcryption, Key Aggregate System are emerged rapidly for better security precaution. It tries to stimulate how to provide authentication in WSN's. Message authentication is the effective ways to find out intruder, unauthorized and corrupted messages from being forwarded in wireless sensor networks .Few message authentication schemes have been developed, which is based on either public-key cryptosystems or symmetric-key cryptosystems. These have little but limitations of high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. A polynomial-based scheme was newly introduced, this scheme have some weakness of a built-in threshold determined by the degree of the polynomial: when the number of messages transmitted is larger than this threshold, it can completely recover the polynomial. In this, we proposed authentication scheme based on elliptic curve cryptography. While permitting intermediate nodes authentication, in our proposed scheme it allows any node to transmit a number of messages without suffering the threshold problem. Our scheme can also provide message privacy. Our proposed scheme is efficient than the polynomial-based approach under comparable security levels while providing message source privacy.**

***Keywords*— Hop-by-hop authentication, symmetric-key cryptosystem,, public-key cryptosystem , source privacy, wireless sensor networks (WSNs),Elliptic curve cryptography(ECC).**

I. INTRODUCTION

The System which permits the sender to send a message to the receiver in that way if modified message will almost detected by Receiver that called as message authentication. Message authentication plays a key role in finding unauthorized illegal and corrupted messages which are forwarded in WSNs. This provide message authenticity and integrity verification for WSNs, scheme categorized into two approaches. First is symmetric key based approach, which are limited to high computational over head and lack of scalability and resilience to node compromise attack though the sender and receiver can be used a shared secret key. The sender uses a shared key to generate Message Authentication Code (MAC) for each transmitted message, But, in this method authenticity and integrity of message can detected by node with the share key, it normally shared by group of sensor node. To tackle this scalability problem a polynomial based message authentication scheme was recently introduced. But it has drawback of a build in threshold which is determined by degree of polynomial l,the number of message is transmitted is larger than that of threshold ,the polynomial can be fully recovered and system will be broken completely. However, alternate solution to find the intruder from recovering the polynomial by computing coefficient of that polynomial. It introduces a perturbation factor; it can not be solved easily. On the other hand, public based approach each message transmitted with digital signature of message – which is generated by using sender private key. The message can be authenticated by every forwarder and final receiver using sender public key, The public key approach have simple and clean key management. But, it has a limitation, is high computation so, recently progressed on ECC. So it can be more advantageous over computation complex and more usage and secure resilience. In this paper, we proposed a one scheme as message authentication as SAMA (source Anonymous Message Authentication) which is based upon Modified ElGamal Signature (MES) Scheme based on elliptic curve .The MES can be secure against adaptive chosen message attack in random oracle model. Our scheme can be enabled the intermediate node to authenticate the message. Our proposed scheme is more efficient than polynomial based algorithm.

The major contribution of paper as,

1) We developed a SAMAC on elliptic curve which provide unconditional source anonymity.
2) We offer a hop by hop message e authentication mechanism for WSNs with limitation of threshold.
3) We devicea N/W on source node privacy protection in WSNs.
4) We proposed efficient key management framework for ensure isolation of compromised node.

This is the first scheme that provide hop by hop node authentication without limitation of threshold and give better performance than symmetric key based approached.

II. TERMINOLOGY

Privacy is generally called as anonymity .communication anonymity in information management was discussed in previous [7], [8], [9], [10], [11], [1]. The state unidentifiable in the set of subject called as sender anonymity, which consist of particular message which not linkable to sender and no message link to one sender. The unconditional secure SAMA definition, Definition 1 (SAMA). A SAMA consists of two algorithms:

• Generate (m;Q1;Q2; · · · ;Qn): here m is a given message and Q1;Q2; · · · ;Qn is the public keys ,S ={A1;A2; · · · ;An}of AS, At the actual message sender ; $1 \leq t \leq n$,) using its own private key dt It produced anonymous message S(m).

• Verify S(m): Here m is message and S(m)is an anonymous Message, which consist of public keys of members in the AS.

The security requirements for SAMA consist:

• Sender ambiguity:-The probability determines the actual sender anonymous message is exactly 1=n, where n is the total members in the AS.

• Unforgeability:- The scheme is unforgeable, public keys of Members of the AS and m1;m2; · · · ;mn message randomly chosen by the adversaries ,from this it produced polynomial time.

Modified ElGamal Signature Scheme:

Definition 2 (MES).MES [1] itconsist of 3 algorithm,

1)Key generation algorithm: here ,p be prime and g be be a generator of Z_P^* ,Both keys are public. private key x $\in$Zp, y is calculated from $y = g^X \bmod p$.

2) Signature algorithm: For ability, it describe variant[13][14], called as optimal scheme. If it signs a message m, one can selects a random $k \in Z^*p-1$, then calculates the exponentiation,

$r = g^K \bmod p$

and s is calculates from:

$s = rxh(m,r) + k \bmod (p - 1)$…..... (1)

where h is a one-way hash function. Signature of messagem is defined as the pair (r; s).

3)Verification algorithm:-The verifier checks the signature Equationgs $= ry^{rh(m,r)} \bmod p$: If it correct, then the verifier Accepts the signature and on the other hand it Rejected .

III. RELATED WORK

The polynomial-based message authentication scheme gives theoretic security with the ideas same as to threshold secret shared scheme, where the degree of the polynomial can be determine its threshold. Messages transmitted are below threshold value, and then it enables the intermediate node to verify the authenticity of the message through polynomial. Since, large amount of messages is transmitted larger than the threshold then polynomial completely recovered and the system will be broken. Perturbation factor was added to the polynomial [2]to increase the threshold and the complexity for the intruder to break the polynomial and noise. The main idea is to find the adversary for computing the coefficient of the polynomial. On the other hand , perturbation factor can be completely removed using error-correcting code techniques [3].Recently, on elliptic curve cryptography (ECC) it shows that the public-key schemes can be more efficient in terms of memory usage, complexity, and security resilience since public-key-based approaches have simple and clean key management [4]. The similar existing communication protocols are largely stemmed from mix net [5] that provides security via packet re-shuffling through a set of mix servers (with at least one being trusted).Now a days, message sender security based on ring signatures was introduced [6]. This public key based approach enables the message sender to generate a source-anonymous message signature with content of a authenticity assurance.

IV. PROPOSED SOURCE ANONYMOUS MESSAGE AUTHENTICATION (SAMA) SCHEME

In this, we propose an unconditionally secure and efficient SAMA. our design enables the SAMA to verify through a single equation without individually verifying the signatures.

A. Proposed MES Scheme on Elliptic Curves:

Consider p > 3 be anodd prime. An elliptic curve E is defined by an equation of the form:

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

where a, b belong 2 Fp, and $4a^3+27b^2 \neq \bmod p$. The set $E(F_P)$ contains all points $(x,y) \in F_p$ on the curve; O is called the point at infinity.

Let $G=(x_G,y_G)$ be a base point on $E(F_p)$ whose order has N which is a large value. User A canselects a random integer as $dA \in [1,N-1]$ as his private key. Then, he can compute his public key Q_A from $QA=d_A \times G$.

Signature generation algorithm. For intruder to sign a message m, follows these steps:

1. Select a random integer kA, $1 \leq k \leq N-1$.
2. Calculate $r = x_A \bmod N$, where $(x_A,y_A) = .k_AG$ If r =0, go back to step 1.
3. Calculate $h_A \xleftarrow{l} h(m,r)$ where h is a cryptographic hash function, such as SHA-1, and $\xleftarrow{l}$ denotes the l Leftmost bits of the hash.
4. Calculate $s = rd_Ah_A+k_A \bmod N$. If s= 0, go back to step 2
5. The signature is the pair (r,s).

Signature verification algorithm. For Bob to authenticated the Signature of Alise's, he should copy her public key QA, then he:

1. Checks that $QA \neq O$, otherwise invalid
2. Checks that QA lies on the curve
3. Checks that $nQA \neq O$ After Bob follows these steps to verify the signature:
1. Verify that r and s are integers in [1,N – 1]. The signature is invalid, if not.
2. Calculate $hA \xleftarrow{l} h(m,r)$, where h is the same function used in the signature generation.
3. Calculate $(x1,x2) = sG - rh_AQ_A \bmod N$.
4. The signature is valid if $r = x1 \bmod N$, invalid

otherwise.
In fact, if the signature is generated correctly then:
$(x1,x2) = sG - rh_AQ_A$
$=(rd_Ah_A+ k)G– rh_AQ_A$
$=k_AG + rh_AQ_A – rh_AQ_A$
$=k_AG$

So, we have x1= r, and the verifier should Accept the signature.

B. Proposed SAMA on Elliptic Curves:

Suppose, the message sender i.e Alice wishes to transmit a message m randomly from her network node to any other nodes. AS includes n members, A1;A2; . . .;An, for example, S {A1,A2,. . .An}, where the actual message sender Alice is A_t, for some t,1≤ t ≤ n. In this paper, could not distinguish between the node Ai and its public key Qi. we also have,
S = {Q1,Q2 . . .Qn).
Authentication generation algorithm. Let m is a message to be transmitted. Sender Alice uses the private key as dt; 1 ≤ t ≤ N. To generate an efficient SAMA for message m, Alice performed the following three steps:
1. Select a random and pair wise different ki for each 1≤ t ≤ N and compute ri from $(r_i,y_i)=k_iG$.
2. Choose a random ki € Zp and compute r_t from $(r_t,y_t)=k_tG - \sum_{I \neq t} r_ih_iQ_i$ such that rt≠ 0 andr_t≠ ri for any i ≠ t; where $h \xleftarrow{l} h(m,r_i)$.
3. Compute $s= k_t + \sum_{i \neq t} k_t+r_td_th_t \bmod N$ .The SAMA of the message m is defined as:
$S(m)=(m ,S ,r_1,y_1,\ldots..,r_n,y_n,s)$.

C: Verification of SAMA

Verification algorithm. For Bob to verify an alleged SAMA $(m.S,r_1,y_1,\ldots.r_n,y_n,s)$ must have a copy of the public keys Q1, . . .,Qn. Then Bob:
1. It Checks that Qi ≠O; i= 1; . . . ; n, otherwise invalid
2. It Checks that Qi, i =1; . . . ; n lies in the curve
3. It Checks that nQi= O; i=1; . . . ; n
After that, Bob follows these steps:
1. Verify that r_iy_ii= 1; . . . ; n,s are integers in[1;N -1]. If is not equal then the signature is invalid.
2. Calculate hi $\xleftarrow{l}$ h(m.r_i), where h is the same function used in the signature generation.
3. Calculate $(x0, y0)=sG -\sum^{n}_{i=1} r_ih_iQ_i$
4. The signature is valid if the first coordinate of $\sum (r_i,y_i)$ equals x0, otherwise it invalid .

To select the proper AS ,it plays a key role in message source privacy. so, in the AS the actual message source node will be hidden .In can prevent the adversaries from finding the message source through the AS analysis with the local traffic analysis. Message source node selects an AS from the public key list in the SS as its choice before a message is transmitted .When an adversary received a message, he could be finding the direction of the previous hop or the real node of the previous hop. On the other hand,if the adversary is does not able to manage the traffic of the previous hop, then he would be unable to differentiate whether the previous node is the actual source node or forwarder node. So, the selection of the AS should create sufficient diversity so that it is infeasible for the adversary to find the message source based on the selection of the AS itself.

V. PERFORMANCE ANALYSIS

In performance analysis, there are two types of analysis, as theoretical and simulation our proposed scheme depend on these both analysis .we are comparing our proposed scheme with the polynomial-based symmetric-key scheme is described in [2]. The comparison of our proposed scheme and thescheme proposed in [2] must be performed with n = 1A. In theoretical Analysis, the secret polynomial is defined as [1]:

$$f(x, y) = \sum_{i=0}^{dx} \sum_{j=0}^{dy} A_{i,j} x^i y^j$$

Where coefficient is $A_{x,y}$is an element of a finite field F*p*,and *dx* and *dy*are the degrees of polynomial. *dx*and *dy*are related to length of message and the computational complexity of scheme. .However, easy to see that the intruders can recover the polynomial *f*(*x; y*) via Lagrange interpolation when it more than *dy*+ 1 messages transmitted from the basestation are received and recorded by the intruders, or more than *dx* + 1 sensor nodes have been compromised, In this, the system security is completely broken and can't be used anytime. This property requires *dx* and *dy*to be large for the scheme to be resilient to node compromising attack. On the other hand one solution is based on perturbation of the polynomial was also explored. The main idea is that to add a very few amount of random noise to the polynomial in the original scheme so that the adversaries will no longer be able to solve the coefficients using Lagrange interpolation. this technique has been proved to be vulnerable to security attacks [3] so, the random noise could be removed by using error-correcting techniques from the polynomial ..While hop-by-hop authentication can be done through a public-key encryption system, the public-key-based schemes were considered as not preferred, due to their high computational. However, our research demonstrates that this is not always true, for elliptic curve public-key cryptosystems. In scheme, each SAMA contains an AS of *n* randomly selected nodes that changes for each message. For*n*= 1, our scheme can provide security for the polynomial-based scheme. For *n* >1, we can get extra privacy for source.
Comparability of the Bivariate Polynomial-Based Scheme :

Table 1: The Original Implementation under 8 MHz Mica2 Platform

a)original implementation[4]							
d_x,d_y=3				d_x,d_y=4			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
14.78	1938	5.8	57.89	15.04	2211	7.59	70.8

Table 2: Our Implementation under 4 MHz Telo

Even though, if one message is corrupted but the other messages in the network can be secure. Therefore, *n* can be smaller than the parameters *dx* and *dy*. In fact, a small *n* may provide some source privacy while ensuring high system performance.

VI.CONCLUSION

In this paper, we proposed an efficient SAMA based on Elliptic curve cryptography established that message sender privacy, SAMA could be applied to the any message which provides authenticity for the content of that message. Providing the hop-by-hop message authentication without the weakness of the built in threshold of the polynomial-based scheme. Our proposed a hop-by-hop message authentication scheme which is based on the SAMA. When applied it to WSNs with fixed sink nodes and also discussed some of the possible techniques for node identification.

b)Our implementation

d_x,d_y=3				d_x,d_y=4			
ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)	ROM (KB)	RAM (B)	Sign (ms)	Verf (ms)
13.61	1938	9	108	13.65	2302	11.73	126.93

REFERENCES

[1] 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.

[2] 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.

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

[4]R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[5]T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[6] 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.

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

[8] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1,pp. 65-75, 1988.

[9] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability,Unobservability, Pseudonymity, and Identity Managementa Proposal for Terminology,"literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[10]A. Pfitzmann and M. Waidner, "Networks without User Observability—Design Options.," Proc. Advances in Cryptology (EUROCRYPT),vol. 219, pp. 245-253, 1985.

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

[12]M. Waidner,"Unconditional Sender and Recipient Intractability in Spite of Active Attacks," Proc. Advances in Cryptology (EUROCRYPT),pp. 302-319, 1989.

[13] L. Harn and Y. Xu, "Design of Generalized ElGamal Type Digital Signature Schemes Based on Discrete Logarithm," Electronics Letters,vol. 30, no. 24, pp. 2025-2026, 1994.

[14]K. Nyberg and R.A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem," Proc. Advances in Cryptology (EUROCRYPT), vol. 950, pp. 182-193, 1995.