ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 6, Issue 6, June 2017

ANALYSIS OF ELLIPTIC CURVE CRYPTOGRAPHY TECHNIQUES FOR SECURE ROUTING IN WIRELESS SENSOR NETWORKS

Ms. Sweety Gupta

Abstract—To thwart illegal messages that enter in wireless sensor networks different types of encryption techniques have been developed. In regard to this polynomial based scheme was recently developed in WSN. So usage of this polynomial scheme has reduced due to significant increase of such attacks. To manage such challenges a lot of work has been done. In this paper a novel scheme of source anonymous message authentication has been done. This research paper shows two different types of encryption technique implemented at the transmitter level namely Polynomial encryption standard and SAMA encryption standard. Thus a simple statement could be made in the paper that SAMA has performed better in all regards like energy consumed, delivery ratio and delay in transmission. Another novel parameter has been introduced in duty cycle for calculation of performance for these two schemes.

Keywords— ECC, ElGamal, Polynomial, SAMA, WSN.

INTRODUCTION

This Message authentication assumes a key part in defeating unapproved furthermore, adulterated bundles from being circled in systems to spare valuable sensor vitality. Consequently, numerous plans have been proposed in writing to give message realness and uprightness in system interchanges [1], [2]. These plans will to an excellent extent be separated into public key-based what is a lot of, symmetric-key-based methodologies.

Polynomial-based encryption message validation plan had been presented earlier [1]. The technique of introducing noise which is random in nature termed as perturbation component was being introduced later on to prevent interception of polynomial's co-efficient' by intruder which can leakage of message[2]. According to latest survey this random natured noise can be deleted from this polynomial encryption by employing error-rectifying code approach [3].

So we have implemented source anonymous message authentication encryption standard which uses the principle of robust optimized ElGamal signature standard on elliptic curves. The above proposed standard is robust to all kind of attacks in oracle model [4]. The significant of this paper includes: (i) source anonymous message authentication encryption standard on elliptic curve which gives the unqualified source ambiguity ; (ii) this method attempts effective hop-by-hop message verification component excluding the bias restriction; (iii) the network execution method on source nodule protection security in wireless sensor network's; (iv) this paper gives broad simulation results under MATLAB 2013 on various security levels.

TERMINOLOGY AND PRELIMINARY

A. *Polynomial Scheme*

This segment gives a progression of message verification standard. This research is led developmentally through a few stages: i) the fundamental thought of polynomial-dependent message verification for authenticated send from base station to standard sensor nodes.

Standard-I: A Basic Polynomial standard for Verification of authenticated Message Send by Base Station

This standard, verified the authenticated messages sent from a base station to simple sensor nodes.

Standard Specification:

• *Introduction to Security Server and Base Station.*

In prime field, the server is random picked by polynomial encryption:

$$f(w,z) = \sum_{0 \le i \le d_w, o \le j \le d_z} B_{i,j} w^i z^j , \qquad (1)$$

where every coefficient $B_{i,j}$ is a component of F_q and scheme attributes d_w, d_z are orders of w and z, individually. At that point, the security server initialize the base station with f(w,z) and a protected one-way hash capacity h(.), which could be MD5, SHA, and so on.

• *Preload the Sensor Nodes*. Prior to a sensor node is conveyed, it is preloaded by the security server with:

-a novel identity n, that is a component of F_q.

-polynomial $verf_u(z) = f(u, z)$, which is known as the authentication polynomial function of node n; and

-the safe one-way hash function h(.).

• *Message Send to the Base Station.* Suppose a the base station is sending a message, indicated by m, it consider the consecutive strides to sign m:

- Hash function h(.) is connected on m to get h(m).
- Polynomial f(w,z) can be calculated on z = h(m) so as to obtain a univariate d_w-order polynomial $MAF_m(w) = f(w,h(m))$, which is known as the message verification operat in m.
- Message $\{m,MAF_m(w)\}$ is conveyed, for all $MAF_m(x)$ is expressed as d_w+1 coefficients[5].

• *Message authentication at Sensor Nodes*. At the point with a sensor node having identity n gets message $\{m,MAF_m(w)\}$, it consider the consecutive strides to confirm the validity and integrity of message:

- h(.) is connected to m so as to obtain h(m).
- ver $f_n(z)$ is calculated on z = h(m) so as to obtain $verf_v(n,h(m))$.
- Received $MAF_m(w)$ is calculated on x = n so as to obtain $MAF_m(n)$.
- If ver $f_v(n, h(m))$ is equal to $MAF_m(v)$, the received message is original.

B. *Presumed systems*

WSN system expect with comprises of countless nodes. Every node is an information string and also an information sink, fitted for his corresponding neighborhood specifically. This entire system is completely associated with hop to hop communication. The security server produces, stores and circulates the security results in the system which reduces the system server. But after assignment, sensor nodes can be confiscated but intruder due to which he or she gets whole information stored so far. So these reduced nodes are not capable of providing new public keys which SS or nodes can take.

C. *Terminology*

Security can also be termed as anonymity. It stands for art of unrecognized in the ambiguity set. Anonymity in terms of sender tells that message cannot be linked to sender.

Terminology 1. Source anonymous message authentication comprises as discuss below with calculations:

• *Originate* ($m,Q_1,Q_2,...,Q_n$): Suppose message m , general public keys $Q_1,Q_2,...,Q_n$ of the AS A = {B_1 , B_2 , ... , B_n}, the real message sender B_t, $1 \leq t \leq n$, creates a source message A(m) utilizing its authenticated private key d_t.

• Check A(m): Check the message m and an unknown message A(m), consisting of public keys of all individuals in the ambiguity set, a checker can figure out if A(m) is produced due to parameters in the AS.

The privacy requirements for source anonymous message include:

• Anonymity of generator : The chances of determination sends the unknown authenticated message which is 1/n, n is the aggregate parameters in the AS.

• Unforgetability: The unknown message method can not be remembered provided the public keys of every member and the unknown message m_1, m_2, ..., m_n which are selected by adversary and can generate in polynomial scheme duration with acceptable unknown authenticated message having small outcomes.

RELATED WORK

A hidden polynomial verification technique was introduced[1]. The technique provides message privacy in a similar manner to threshold hidden sharing technique in which threshold can be obtained by order of polynomial. The latest advancement in ECC depicts that the public key technique can prove boon when memory usage, complexity of message is considered. Without ECC the normal public dependent methods are simple and key management is easy [6].

PROPOSED SAMA ENCRYPTION STANDARD

This portion , the robust highly secure and very efficient SAMA encryption technique has been employed. This enables verification of SAMA encryption by individual equation without the need of verifying each signature.

D. Implementation of optimized ElGamal signature with Elliptic Curves

Consider p as an odd number which is prime and greater than 3. The elliptic curve can now be defined by equation:

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

where $a, b \in F_p$, and $4a^3 + 27b^2 \not\equiv 0 \bmod p$. The set $E(F_p)$ comprises of all focuses $(x, y) \in F_p$ on the curve, which consist of unique point O, known as point at limitlessness.

Consider $G = (x_G , y_G)$ as main point on $E(F_p)$ which has large degree N. Client A chooses an irregular number $d_A \in [1,N-1]$ as one private key. At that point, user can process public key Q_A which is $Q_A = d_A \times G$.

Signature process calculation: Bob sign message m in below discuss strides:

1) choose an arbitrary whole number k_A, $1 \leq k_A \leq N-1$.

2) Compute $r = x_A \bmod N$, for which $(x_A , y_A) = k_A G$. In the event that r = 0, backtrack to step 1.

3) Calculate $h_A \xleftarrow{l} h(m, r)$, h is a cryptographic hash capacity, for example, SHA-1, and $\xleftarrow{l}$ where l signifies extreme left bit in hash.

4) Compute $s = rd_Ah_A+k_A \bmod N$. On the off chance that s = 0, perform step 2 again.

5) Pair (r, s) means signature.

While calculating s, string h_A comes from h(m, r) which must be changed to integer.

Signature authentication calculation: Alice can verify Bob's signature if he has replica of public key Q_A, then:

1) Verify $Q_A \neq O$, else this is infeasible.

2) Verify Q_A must be on curve

3) Verify $n Q_A = O$

Then Alice uses following steps for signature verification:

1) Check r and s are whole numbers in $\{1, N-1\}$. otherwise signature is not valid.

2) Compute $h_A \xleftarrow{l} h(m, r)$, in which h is the parameter which was utilized for calculation of signature.

3) Compute $(x_1, x_2) = sG - rh_AQ_A \bmod N$.

4) Signature is authentic if $r = x_1 \bmod N$, otherwise it is not considered.

E. Implementation of source anonymous message authentication with Elliptic Curves

Assume the sender (Bob) sends message m unknowingly to any node from any other node. Ambiguity set incorporates n individuals, $B_1, B_2, ..., B_n$, e.g., $S = \{ B_1, B_2, ..., B_n \}$, in which genuine source of message Bob is B_i.

Calculation of authentication generation: Consider m as transmitted message, in which private key of the Bob is d_t, $1 \leq t \leq N$ who is message sender. For effective SAMA encryption Bob calculates three steps mentioned below:

1) Compute an irregular and distinctive k_i where every $1 \leq i \leq n-1$, $i \neq t$, then calculate r_i from $(r_i, y_i) = k_iG$.

2) Choose an irregular $k_i \in z_p$ and process r_t from $(r_t, y_t) = k_tG - \sum_{i \neq t} . r_ih_iQ_i$

such that $r_t \neq 0$ and $r_t \neq r_i$ for any $i \neq t$; where $h_i \xleftarrow{l} h(m, r_i)$.

3) Calculate $s = k_t + \sum_{i \neq t} k_i + r_td_th_t \bmod N$.

The SAMA of the message m is :

$S(m) = (m, S, r_1, y_1, ... , r_n, y_n , s)$.

F. SAMA Verification

verification calculation*: for Alice to check SAMA(m,S, $r_1, y_1, ... , r_n, y_n, s$), there must be a encrypted keys $Q_1, ..., Q_n$.*
1. Verify $Q_i \neq 0$; i = 1, ... ,n, it is not cosidered.
2. Q_i , i = 1, ... , n must lies on curve
3. $n Q_i = O$, i = 1, ... , n
Then Alice does following steps:
1. Compute r_i, y_i, i = 1, ... , n, and s are integers in [1,N − 1]. Otherwise signature is not considered.
2. Compute $h_i \xleftarrow{l} h(m,r_i)$, h is the function used earlier for origination of signature.

3. *Calculate* $(x_0, y_0) = sG -$
4. *The mark is substantial if the main direction of) meets, invalid it is something else.*

SOURCE SECRECY AND AMBIGUITY SET CHOICE

Ambiguity set's proper election has an important role to play in message secrecy. Prior to message transmission selection of AS is done by node via public key details in SS must have itself and other nodes.

ANALYSIS THROUGHPUT

Evaluation of implemented authentication standard is done via both theoretical and simulated methods. Comparison of implemented technique by polynomial dependent symmetric key[2]. The comparison between both technique is done by considering n = 1.

G. Theoretical Analysis

Hidden bivariate polynomial [1]:

$$f(w,z) = \sum_{i=o}^{d_w} \sum_{j=o}^{d_z} B_{i,j} w^i z^j$$

where every coefficient $B_{w,z}$ is a component of a limited field F_p , d_w and d_z denotes power of polynomial which are associated with length of original message and calculation complexity. For better throughput d_w, d_z must be short.

The system privacy gets shaken when interceptor receives polynomial f(w,z) through Lagrange insertion while d_z+1 number of message are interceptor's and received by d_w+1 nodes. To overcome this d_w and d_z must have large values.

In other scheme small noise was added in polynomial. This is Lagrange interpolation method. In any case this system is demonstrated to be defenseless against security assaults [3]. This method is more easily hacked because noise can be removed via mistake redressing system. Public encryption key is not considered due to high calculation complexity.

In proposed method source anonymous message encryption consists of ambiguity set which has n arbitrary nodes. For n=1, the technique gives similar security as compared to polynomial encryption method. If n>1, source secrecy gets more advantageous.

H. Trial Results

In this segment, we look at the bivariate polynomial-based plan and our plan in view of equivalent security levels.

1. *Simulation parameter setup*: symmetric encryption key is used in polynomial technique; while the implemented technique uses the principle of elliptic curve cryptography. In this basically we require keys of suitable sizes.

Suppose if for symmetric key encryption the size of key is l then for elliptic key cryptography key size will be 2l.

In the implementation simulation five levels of security have been choosen indicated by key size l: 24bit, 32bit, 40bit, 64bit, and 80bit. The key size of proposed technique are 48bit, 64bit, 80bit, 128bit, and 160bit, separately.

We likewise need to decide d_w and d_z for polynomial technique, and the n for proposed technique.

2. *Proposed Work*: To extend the concept of security previously the authors introduced in energy, delay per seconds and throughput as prime parameters for calculations and comparisons. In this research work a new

parameter has been proposed for improving the calculations and research. This parameter is duty cycle which is a novel parameter for calculation of timing triggering of a user transmitting, generating a encrypted message , verifying the received message and calculating the consumed energy.

SIMULATION RESULTS:

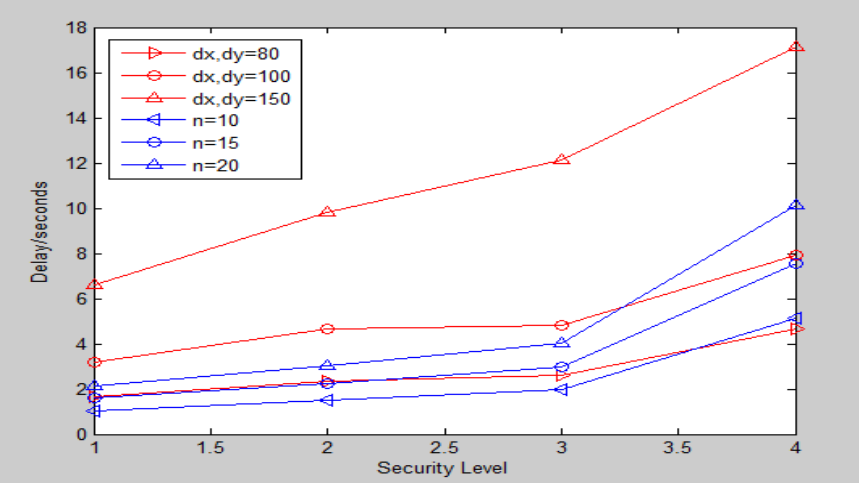

Figure1: Detailed display of delay per second in two techniques using four level l=32, 40,64,80.

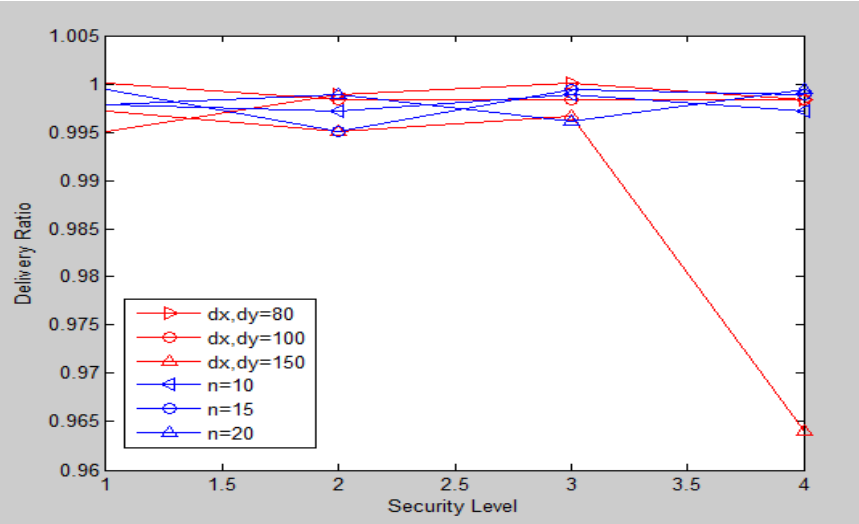

Figure 2: Display of two delivery ratio in the polynomial and proposed scheme again taking four levels of security

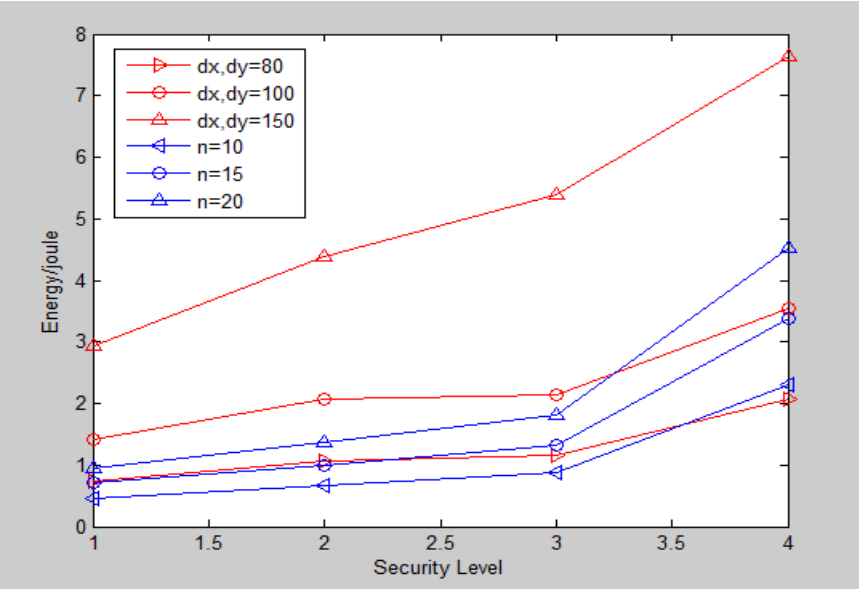

Figure 3. The calculation of energy per unit joule consumed in the polynomial scheme and proposed encryption scheme

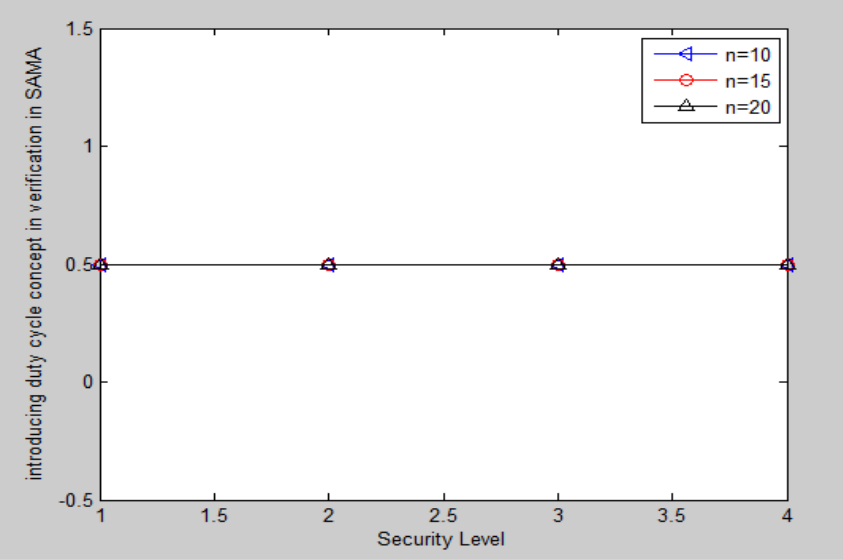

Figure 4. This figure shows a constant verification time with increasing level of security and increasing number of users in proposed scheme

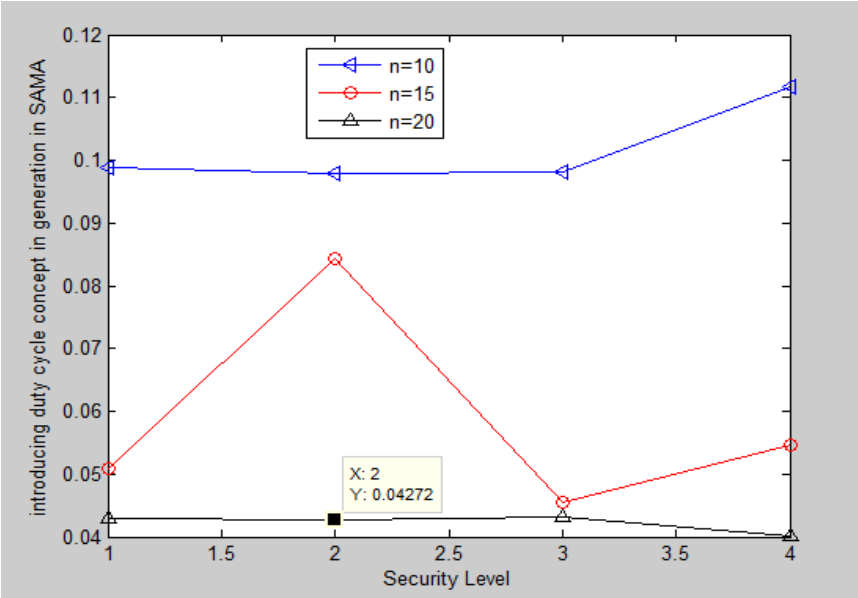

Figure 5: Variation in the duty cycle ratio for increasing level and increasing number of users.

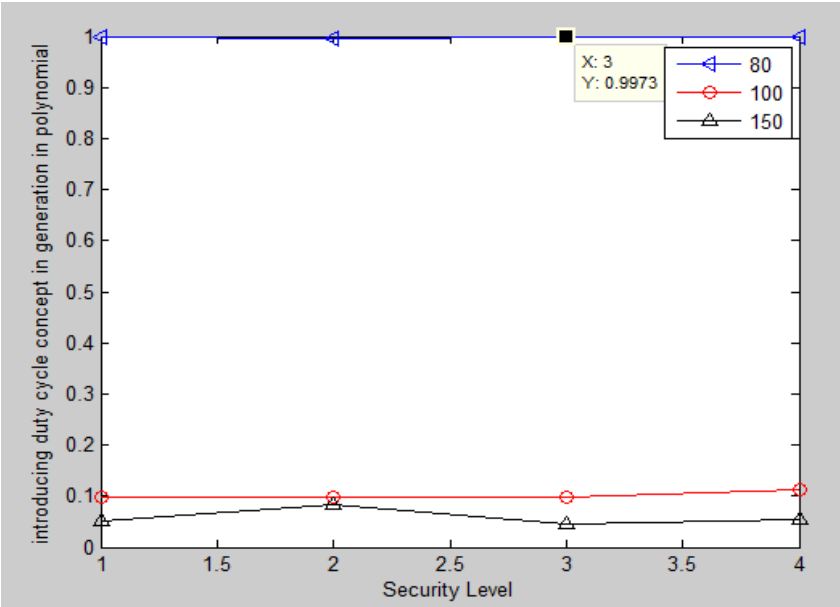

Figure 6: The calculation of polynomial scheme duty cycle at the generation and increasing number of users

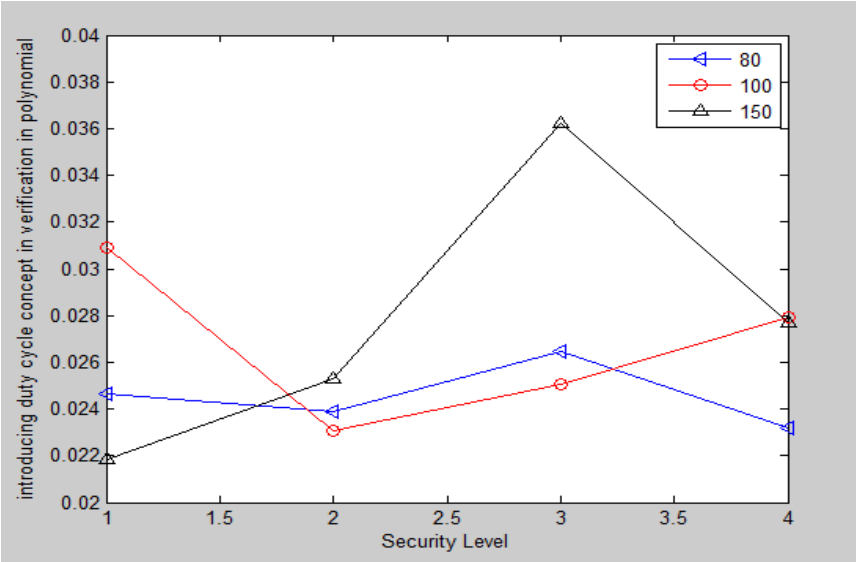

Figure 7: Drastic change in the verification table and its representation in polynomial scheme with increasing users and security level.

TABLE

COMPARSION OF POLYNOMIAL SCHEME AND PROPOSED SCHEME WITH RESPECT TO GENERATION AND VERIFICATION TIME TAKEN IN THE PROCESS FOR DIFFERENT VALUES OF L=24, 32, 40 64, 80.

	Polynomial-based approach						Proposed approach							
	$d_x, d_y = 80$		$d_x, d_y = 100$		$d_x, d_y = 150$		n = 1		n = 10		n = 15		n = 20	
	Gen	Verify	Gen	Verify	Gen	Verify	Gen	verify	Gen	verify	Gen	Verify	Gen	Verify
l=24	6.6493	0.0002	12.7202	0.0002	26.3383	0.0002	0.2248	0.5004	4.1746	2.3769	6.3449	3.4399	8.5439	4.4723
l=32	9.4579	0.0002	18.6351	0.0002	39.3589	0.0002	0.3294	0.7047	5.9870	3.3146	8.9231	5.0181	12.1908	6.8614
l=40	10.4876	0.0002	19.2392	0.0002	40.4473	0.0002	0.4551	1.0329	7.8931	4.4240	11.7977	6.6747	16.2041	8.9001
l=64	18.6329	0.0002	31.7260	0.0002	68.5826	0.0002	1.1757	1.7048	20.6285	11.3779	30.2984	16.8315	40.5027	22.2545
l=80	23.5704	0.0002	38.8238	0.0002	84.9328	0.0002	1.4103	2.1895	26.3457	13.8779	37.5184	20.8183	50.7265	25.7772

CONCLUSION

This research paper has shown a new field of encryption technique in which the security level has been taken to an extreme value.

The complete scenario was developed in MATLAB and SIMULINK version 2013a version. Now if the complete work is scrutinized then first of all a simulation coding setup has been developed for source anonymous message authentication scheme. In this case the user has been taken as n=10, n=15 and n=20. Now if the results are evaluated for energy consumed in SAMA then the graphical results shows that maximum energy will be consumed when number of users will increase. In a similar manner when polynomial encryption scheme is developed then energy consumed increases with number of users. However the results indicate that with increasing number of users SAMA consumes less energy as compared to polynomial scheme.

Similarly when a comparison is drawn between SAMA and polynomial scheme then the delivery ratio is consistent in the SAMA scheme whereas in polynomial scheme the results dips at the highest level of security with increasing users.

Thus a final conclusion can be drawn in this regard that when users are increasing number of users are considered and the security level increases then SAMA will perform better.

Another point to be noted in this regard is that SAMA taken in our discussion has been implemented on the basis of the description given earlier in the previous work.

The duty cycle concept is a novel parameter that adds a new dimension for the calculation of results both at the generation and verification. Observations for figure 6 and 7 shows that polynomial scheme has sudden increase in the duty cycle ratio when increasing users and increasing number of levels. The system level performance of proposed SAMA shows a constant duty cycle with increasing users and level of security.

APPENDICES

AES	Advanced Encryption Standard
AS	Ambiguity Set
DES	Data Ambiguity Set
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
MAF	Message Authentication Function
MES	Modified ElGamal Signature Scheme
SAMA	Source Anonymous Message Authentication
WSNs	Wireless Sensor Networks

REFERENCES

[1] 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.

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

[3] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking cryptographic schemes based on "perturbation polynomials"." Cryptology ePrint Archive, Report 2009/098, 2009. http://eprint.iacr.org/.

[4] 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.

[5] G. Wang. "Lightweight and Compromise-Resilient Message Authentication in SensorNetworks", 2008 Proceedings IEEE INFOCOM -The 27th Conference on Computer Communications, 04/2008.

[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," in IEEE ICDCS, (Beijing, China), pp. 11–18, 2008.

[7] Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].