Circuits and Systems, 2016, 7, 3204-3211
Published Online August 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.710273

Security Implementation in WSN with Symmetric and Matrix Mapping on Asymmetric ECC Cryptographic Techniques

S. Hemalatha[1], V. Rajamani[2], V. Parthasarathy[3]

[1]Department of Information Technology, Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
[2]Department of Electronics & Communication Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
[3]Department of Computer Science & Engineering, Vel Tech Multi Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Chennai, India
Email: hema.vtht@gmail.com, rajavmani@gmail.com, sarathy.vp@gmail.com

Received 5 May 2016; accepted 15 May 2016; published 23 August 2016

Abstract

As the wireless sensor networks are easily deployable, the volume of sensor applications has been increased widely in various fields of military and commercial areas. In order to attain security on the data exchanged over the network, a hybrid cryptographic mechanism which includes both symmetric and asymmetric cryptographic functions is used. The public key cryptographic ECC security implementation in this paper performs a matrix mapping of data's at the points on the elliptical curve, which are further encoded using the private symmetric cipher cryptographic algorithm. This security enhancement with the hybrid mechanism of ECC and symmetric cipher cryptographic scheme achieves efficiency in energy conservation of about 7% and 4% compared to the asymmetric and symmetric cipher security implementations in WSN.

Keywords

WSN, Security, Elliptic Curve Cryptography, Symmetric Cipher Cryptography, Hybrid Cryptosystem, Matrix Mapping

1. Introduction

The use of wireless sensor network has been evolved in practise due to the inconvenience of using the wired

How to cite this paper: Hemalatha, S., Rajamani, V. and Parthasarathy, V. (2016) Security Implementation in WSN with Symmetric and Matrix Mapping on Asymmetric ECC Cryptographic Techniques. *Circuits and Systems*, **7**, 3204-3211. http://dx.doi.org/10.4236/cs.2016.710273

technology. With the development in network and communication technology, WSN is used in wide areas such as remote sensing, health monitoring, industrial process monitoring, military and various commercial applications. WSN has the ability to balance the harsh environmental conditions, node failures during transmission, scalability of large scale deployment and etc. This network faces the problem of high energy consumption during communication. And various techniques were proposed to conserve energy among the sensors in the network.

Since the sensors are highly involved in data transmission and reception, they pave ways for the attackers to inject suspicious bits into the original message, eaves drop the messages and inhibit various other threat and attacks that affects the confidentiality, integrity and authenticity of the original plaintext [1]. The security in WSN can also be affected by deploying malicious nodes in the network which may either be purchased or by converting the available nodes into malicious one. This may affect the entire system process cooperatively. This paper works on to secure the data exchanged between the nodes in the network.

The data transmission security is commonly achieved through cryptography in WSN. Cryptography secures the data through the encryption and decryption [2]. It consists of two categories: Symmetric and asymmetric cryptography, where a single key is used to perform the security operation in the former method and two different keys are used in the later method. Various cryptographic algorithms are proposed to achieve security. The cryptographic algorithms functions with the generation of the key which ensures the secrecy of the messages.

The elliptic curve cryptographic technique follows a public key mechanism, which uses different keys for encryption and decryption process [2]. The reason to use ECC is that, it achieves the same security level offered by other security techniques but with smaller key size. Moreover, it requires reduced storage and transmission requirements. This ECC is said to be more efficient among all the public key cryptographic techniques and especially the RSA method because, the same level of security but with smaller key size is provided by ECC through which efficiency in bandwidth, storage and transmission can be achieved.

The authors Hemalatha and Rajamani [3] proposed an effective WSN by assuring security during the communication. They achieved security by deriving from the ancient Indian Vedic mathematics. The authors explained that, the cross multiplication behaviour of the Vedic mathematics when applied to the places where point multiplications are available, a cost effective and improved information security can be obtained.

In order to provide a high degree of security for WSN, the author Oreku [4] presented a WSN reliability mathematical calculation approach. This technique gives an idea on how to secure WSN through reliable backbone connectivity, reliable sensor network and data aggregation. A technique based on security broadcast with linear network coding, shortly called SBLNC was proposed by the author Zhenjiang Zhu [5] *et al*. The proposed coding method can improve the throughput of the broadcasted messages, reduce the energy consumption and delay of the node thereby solving the security problems in the network.

An Elliptic curve cryptography, another public key cryptographic (PKC) algorithm providing same level of security as the RSA but with smaller key size requirements, was used by the author Kodali [6] as an alternative to RSA to provide security in WSN applications, where elliptic points are produced to carryon the process. The authors Xu Huang and Sharma [7] proposed a technique where the key calculation time in the security mechanism can be reduced. Since the ECC scalar multiplication takes about 80% of key calculation time on WSN, a fuzzy controller for dynamic window that allows the calculation to be processed under an optimum condition was developed by the authors.

In order to exchange the data among the nodes and the base station in WSN in a secure manner, the authors Kodali and Budwal [8] implemented the usage of ECC. Since ECC requires higher key calculation time, they proposed an optimized Sliding Window method with 1's complement technique for scalar multiplication and compared the results with Binary Method and Non-Adjacent Form (NAF) method of scalar multiplication.

Since the security and excessive power consumption of WSN is becoming the major concerns in recent times, the authors Xu Huang [9] *et al*. proposed an optimized dynamic window technique which reduced the power consumption in the ECC wireless sensor network. And they further reduced the average key calculation time to about 18% compared to the previous results. The authors Zhang [10] *et al*. proposed a symmetric cryptographic mechanism to achieve security with reasonable energy consumption in WSN. A block cipher symmetric cryptographic scheme referred to as byte-oriented substitution-permutation network (BSPN) mechanism was proposed to reduce energy consumption and achieve security in the wireless sensor network.

Since the ECC security mechanism over the messages can be achieved at the elliptic curve points, this paper follows a new matrix mapping mechanism [11] [12], followed by the encoding and decoding functions using the symmetric cipher algorithm, which is explained in detail in the following sessions. This paper achieves security on the messages exchanged between the sensors in the network by implementing a combination of public and private cryptographic techniques. The ECC public cryptographic mechanism maps the alphanumeric characters of the text onto the point on the elliptic curve. Further, these mapped points are encoded and decoded using a symmetric block cipher mechanism.

The rest of the section is organized as follows: Section 2 outlines the procedure to process the proposed functions, the results are analysed in Section 3 and finally the Section 4 concludes the proposed work.

2. Security Enhancement over WSN

In order to ensure security during the data transmission among the sensor nodes in WSN, a public key cryptographic algorithm and a symmetric cipher functions to encode and decode the mapped points on the elliptic curve are used in this paper. Since elliptic curve cryptographic algorithm offers equal security with smaller key size thus reducing the bandwidth and computational complexity compared to RSA, ECC is preferred among all the public key cryptographic techniques.

The following sections explain the procedure to implement the security on the transmitted data over the network.

2.1. Point Generation on the Elliptic Curve

With the elliptic curve points, operations such as point inverse, point addition, subtraction, and multiplication can be performed. Let a finite field F_b define an elliptic curve $r_2 = s_3 + as + b$, where the two non-negative integers "*a*" and "*b*" are less than the prime "*p*" The points on the elliptic curve can be obtained by computing $r_2 = s_3 + as + b$ (*mod p*) for the value of "*r*" varying from 0 *to p* initially, and $r_2 = s_3 + as + b$ (*mod p*) for "*s*" varying from 0 *to p*. If the match is obtained on caparison for the values obtained from r_2 for *s* and *r*, then *s* and *r* will be the point on the elliptic curve for which the inverse will also be present on the curve. Once the points are generated on the curve, they further undergo a matrix mapping mechanism which is explained in the next session (**Figure 1**).

Where $-p(s_1, r_1)$ is the inverse on the elliptic curve for the point $p(s_1, r_1)$, which can be computed by performing the following substitution

$$-p(s_1, r_1) = p(s_1, p - r_1) \quad (1)$$

2.2. Matrix Based Point Mapping Mechanism

Mapping can be done in static method and dynamic method [13]. The secrecy of the transmitted message by the static method cannot be maintained, since it can pave way for the intruder to interpret the data by trial and error method. Therefore, dynamic mapping method is preferred, where the alphanumeric characters are dynamically mapped onto the points of the elliptic curve.

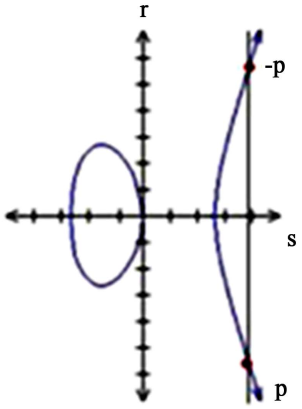

Figure 1. Point Inverse operation.

Let the finite field F_b holding the elliptic curve contain the set of elliptic points and its base point generated known publicly. The ASCII values of each character of the exchanged messages among the nodes in the wireless sensor network are mapped to the points that are generated on the elliptic curve. The mapping is performed as explained below:

STEP 1: The alphanumeric values of each character in the transmitted message should be transferred into their respective ASCII values.

STEP 2: A scalar value that represents the derived ASCII value of the character should undergo a point multiplication with the base point in the elliptic curve. For instance, if *x* represents a scalar value, then a point multiplication of "*x* * *p*" should be performed. This process should be repeated for all the characters in the string.

STEP 3: A "2 × *b*" matrix "*R*" should be constructed with the entries of the generated elliptic curve points.

$$R = \begin{bmatrix} p_1 & p_2 & p_3 & \cdots & p_a \\ p_{a+1} & p_{a+2} & p_{a+3} & \cdots & p_b \end{bmatrix} \tag{2}$$

If *n* is the length of the original message then *a* = *n*/2. The space will be represented by the points on the curve that are padded with *α*.

STEP 4: A 2 × 2 non-singular matrix "*S*" is chosen as $S = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ and a 2 × 2 matrix *T* is constructed with a mathematical entries of sequence k_n.

$$T = \begin{bmatrix} k_1 p & k_2 p & k_3 p & \cdots & k_a p \\ k_{a+1} p & k_{a+2} p & k_{a+3} p & \cdots & k_b p \end{bmatrix} \tag{3}$$

STEP 5: Finally, the resultant mapped points can be obtained by constructing "*U*" with the point multiplication and addition process, represented as *U* = *RS* + *T*, resulting in

$$U_i = \left[U_i \left(x_i, y_i \right) \right] \tag{4}$$

where,

$$U = \begin{bmatrix} U_1 & U_2 & U_3 & \cdots & U_a \\ U_{a+1} & U_{a+2} & U_{a+3} & \cdots & U_b \end{bmatrix} \tag{5}$$

Once all the alphanumeric characters of the message string are mapped onto the constructed elliptic curve, the mapped points will further be encoded using the symmetric cipher algorithm, which is explained in detail in the next section. The transmitted original message will be retrieved by decoding the message with the symmetric cipher key used to encode the plaintext, followed by the inverted matrix mapping mechanism.

2.3. Symmetric Cipher Encoding and Decoding Operation

In order to make the message non-readable for the opponent, a symmetric cipher security technique which conserves energy in the WSN is used to encode and decode the mapped message at the point on the curve (**Figure 2**).

ENCODING

STEP 1: The ASCII value of the alphanumeric character should be generated and their respective binary value should be produced.

STEP 2: Divide the reversed form of the 8 bit binary number generated in step1 with a 4 bit divisor key.

STEP 3: The 8 bit encrypted text should be stored as, the remainder in the first 3 digit and the quotient in the following 5 digit.

DECODING

The encrypted 8 bit cipher text undergoes the below mentioned steps to retrieve the transmitted original message.

STEP 1: The last 5 digit binary value of the encrypted cipher text should undergo a multiplication with the 4 bit symmetric key.

STEP 2: The result obtained in step 1 should be added with the first 3 digits of the encrypted cipher text which forms an 8 bit number.

STEP 3: The transmitted original plaintext can be obtained by reversing the 8 bit digit in step 2.

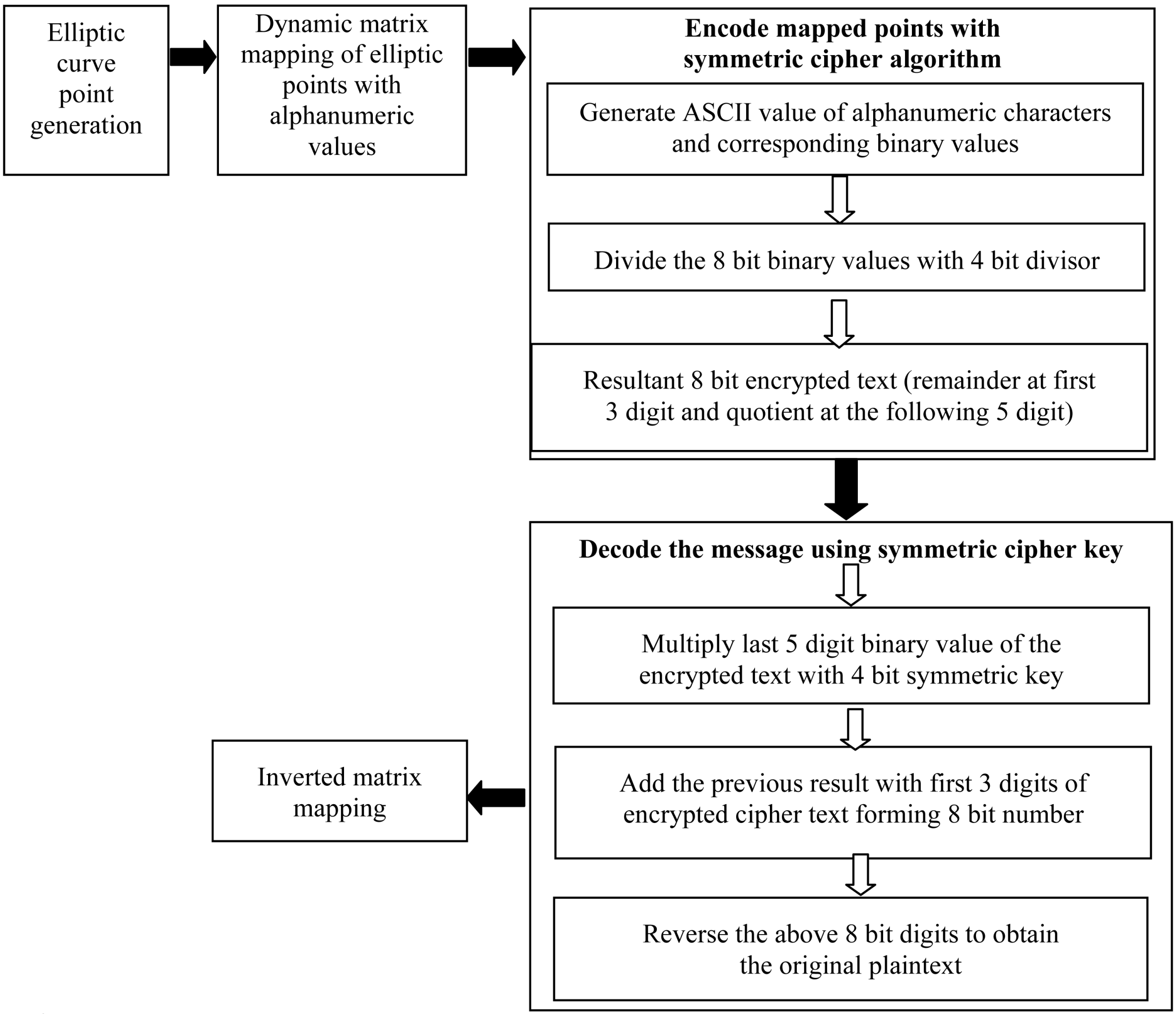
Elliptic curve point generation
Dynamic matrix mapping of elliptic points with alphanumeric values
Encode mapped points with symmetric cipher algorithm
Generate ASCII value of alphanumeric characters and corresponding binary values
Divide the 8 bit binary values with 4 bit divisor
Resultant 8 bit encrypted text (remainder at first 3 digit and quotient at the following 5 digit)
Decode the message using symmetric cipher key
Multiply last 5 digit binary value of the encrypted text with 4 bit symmetric key
Add the previous result with first 3 digits of encrypted cipher text forming 8 bit number
Reverse the above 8 bit digits to obtain the original plaintext
Inverted matrix mapping

Figure 2. Security implementation block diagram.

3. Result and Analysis on the Proposed Hybrid Cryptosystem

This section presents a comparative analysis on the energy consumption by the nodes in WSN, among the asymmetric, symmetric and the hybrid cryptographic security implementation. The comparison is done at the intermediate nodes, source nodes, destination nodes and the overall energy consumption in the network.

The experimentation is carried with varying message size of 1024, 2048, 4086 and 8192 bytes on the Atmega 128 16 MHz 8 bit architecture instruction set. The experimentation will start with the basic implementation of sensor network in OPNET Modeler Simulator. Sensor field will be used as logical area with various sensor nodes. We start our proceeding with pre deployment of sensor nodes and continue with implementation of traffic on sensor network. Later the pre-defined asymmetric keys will be distributed to all the sensor nodes. This key distribution will inhibit public encryption to the deployed network. Energy will be measured and must be more than threshold energy level. For the complete segregation of the users, we will use MD5 algorithm at login of the query initiation process which will be processed for ECC encryption further.

Figure 3 compares the energy consumption at the intermediate nodes. The energy consumption in the proposed scheme is found to be 8% lesser than the asymmetric method and 6% lesser than the symmetric cryptographic security scheme. The key idea behind this improvement is that it uses the efficient asymmetric ECC cryptographic method to map the alphanumeric characters of the transmitted message on the elliptic points which will implement the security before it enters into the next level of security implementation through the encoding operation using the symmetric block cipher cryptographic mechanisms. As the proposed asymmetric cryptographic method is efficient in storage and transmission requirements due to its smaller key size, and the symmetric method is efficient in conserving energy among the sensors during transmission, the entire proposed scheme is found to reduce the energy consumption greatly.

Figure 4 denoting the energy consumption at the source node proves that the proposed technique consumes energy to about 7% lesser than the asymmetric and 5% lesser than the symmetric cryptographic security mechanism. **Figure 5** explains the amount of energy consumed by the sink node with the proposed security mechanism. Here the sink node is found to consume energy of about 6% lesser and 3% lesser than the asymmetric and symmetric security methods. And the overall energy consumption by the proposed technique is found to be 7% lesser and 4% lesser than the asymmetric and symmetric security schemes, which is denoted in **Figure 6**.

4. Conclusion

A hybrid cryptographic security mechanism including both symmetric and asymmetric cryptographic techniques is used in this paper to achieve security to maintain the confidentiality, integrity and authenticity of the messages exchanged among the sensors in WSN. The usage of public elliptic cryptography method achieves bandwidth and transmission efficiency due to its smaller key size. The matrix based mapping methodology maps all the alphanumeric characters at the point on the elliptic curve thereby securing the secrecy of the message highly. These

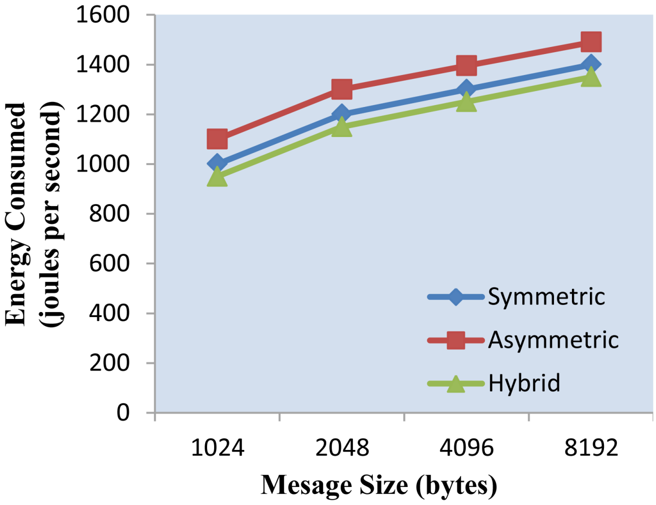

Figure 3. Intermediate nodes energy.

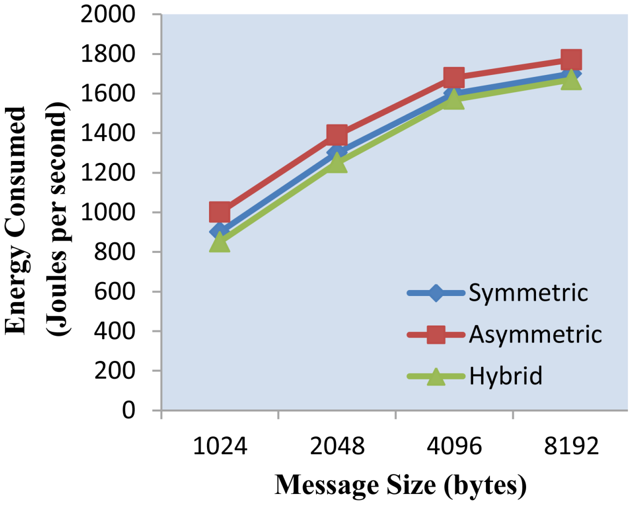

Figure 4. Energy consumption at source node consumption.

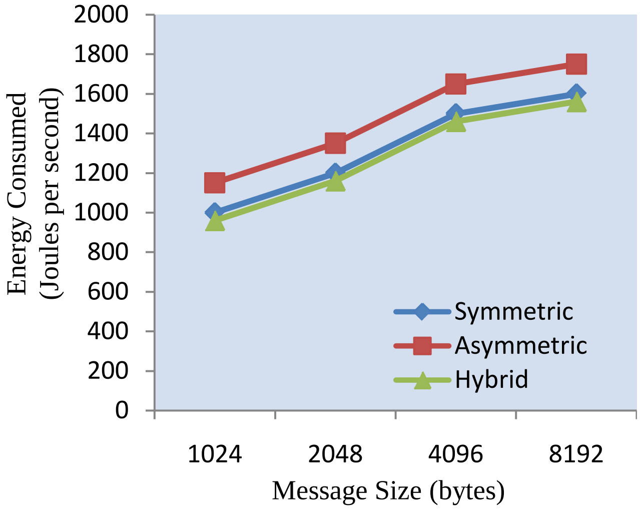

Figure 5. Energy consumption at sink node.

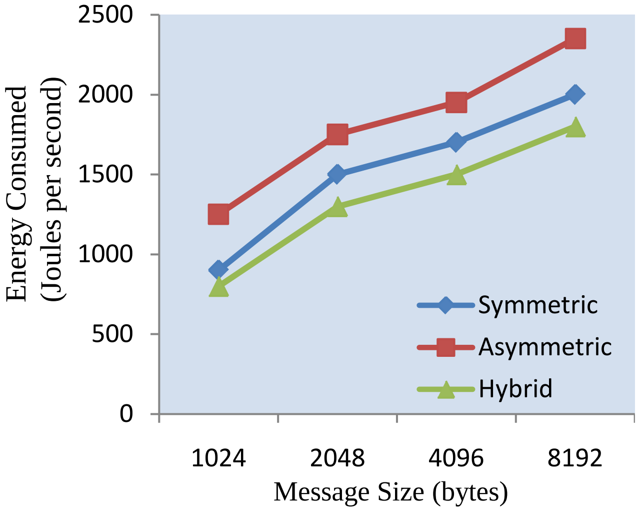

Figure 6. Overall energy consumed in WSN.

points are finally encoded using the symmetric cipher method. This proposed hybrid security scheme results in the overall energy conservation of about 7% and 4% compared to the individual asymmetric and symmetric cryptosystems in WSN. This work can further be enhanced with factors like lifetime of Sensor nodes, data-block size and transmission range in the network.

References

[1] Walters, J.P. and Liang, Z.Q. (2006) Wireless Sensor Network Security: A Survey. *Security in Distributed, Grid, and Pervasive Computing*.

[2] Oswald, E. (2005) Introduction to Elliptic Curve Cryptography. *Institute for Applied Information Processing and Communication*.

[3] Hemalatha, S. and Rajamani, V. (2014) VMIS: An Improved Security Mechanism for WSN Applications. *International Conference on Science Engineering and Management Research* (*ICSEMR*). http://dx.doi.org/10.1109/ICSEMR.2014.7043667

[4] Oreku, G.S. (2013) Reliability in WSN for Security: Mathematical Approach. *International Conference on Computer Applications Technology* (*ICCAT*). http://dx.doi.org/10.1109/iccat.2013.6522041

[5] Zhu, Z.J., Tan, Q.P., Zhu, P.D. and Zheng, Q.B. (2008) Security Broadcast Based on Linear Network Coding in WSN.

International Conference on Computer Science and Software Engineering. http://dx.doi.org/10.1109/csse.2008.676

[6] Kodali, R.K. (2014) ECC with Hidden Generator Point in WSNs. IEEE Conference Publications. http://dx.doi.org/10.1109/tenconspring.2014.6863011

[7] Xu, H. and Sharma, D. (2010) Fuzzy Controlling Window for Elliptic Curve Cryptography in Wireless Networks. 5*th International Conference on Computer Sciences and Convergence Information Technology* (*ICCIT*). http://dx.doi.org/10.1109/ICCIT.2010.5711111

[8] Kodali, R.K. and Budwal, H.S. (2013) High Performance Scalar Multiplication for ECC. *International Conference on Computer Communication and Informatics* (*ICCCI*). http://dx.doi.org/10.1109/iccci.2013.6466286

[9] Xu, H., Sharma, D., Aseeri, M. and Almorqi, S. (2011) Secure Wireless Sensor Networks with Dynamic Window for Elliptic Curve Cryptography. *Saudi International Electronics*, *Communications and Photonics Conference* (*SIECPC*). http://dx.doi.org/10.1109/siecpc.2011.5877000

[10] Zhang, X.Y., Heys, H.M. and Li, C. (2010) Energy Efficiency of Symmetric Key Cryptographic Algorithms in Wireless Sensor Networks. 25*th Biennial Symposium on Communications* (*QBSC*). http://dx.doi.org/10.1109/bsc.2010.5472979

[11] Amounas, F. and El Kinani, E.H. (2012) Fast Mapping Method Based on Matrix Approach for Elliptic Curve Cryptography, Moulay Ismaïl University, Morocco. *International Journal of Information & Network Security* (*IJINS*), **1**, 54-59.

[12] Geetha, G. and Jain, P. (2014) Implementation of Matrix Based Mapping Method Using Elliptic Curve Cryptography. *International Journal of Computer Applications Technology and Research*, **3**, 312-317.

[13] Srinivasa Rao, O. and Setty, S.P. (2010) Efficient Mapping Methods for Elliptic Curve Cryptosystems. *International Journal of Engineering Science and Technology*.