International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-7, Issue-8)

Research Article | **August 2017**

Enhanced Security Authentication of WiMAX using EC^{3}A

Mohd Javed, Khaleel Ahmad, Ahmad Talha Siddiqui
Department of CS & IT, MANUU, Hyderabad,
Telangana, India

DOI: 10.23956/ijarcsse/V7I7/0102

Abstract—WiMAX is the innovation and upgradation of 802.16 benchmarks given by IEEE. It has numerous remarkable qualities, for example, high information rate, the nature of the service, versatility, security and portability putting it heads and shoulder over the current advancements like broadband link, DSL and remote systems. Though like its competitors the concern for security remains mandatory. Since the remote medium is accessible to call, the assailants can undoubtedly get into the system, making the powerless against the client. Many modern confirmations and encryption methods have been installed into WiMAX; however, regardless it opens with up different dangers. In this paper, we proposed Elliptic curve Cryptography based on Cellular Automata (EC^{3}A) for encryption and decryption the message for improving the WiMAX security

Keyword--- IEEE 802.16, WiMAX, ECC, CA, Encryption, Authentication

I. INTRODUCTION

WiMax (Worldwide Interoperability for Microwave Access) is portrayed as "a standard based innovation, empowering the conveyance of last mile remote broadband accesses as another option to link and DSL" [1].

It offers numerous elements with a great deal of adaptability and has supplanted a hefty portion of the current media transmission advancements [2]. WiMAX is the exchange name of IEEE 802.16 set up by an IEEE standard board in 1999 [3]. Three working gatherings of the IEEE have been diagrammed to create a standard:

- IEEE 802.16.1- Air interface for 10 to 60 GHz.
- IEEE 802.16.2-Co-existence of broadband wireless access systems.
- IEEE 802.16.3-Air interface for licensed frequencies, 2 to 11 GHz.

The security has become a primary concern in order to provide protected communication between a wireless environment [2]. Security in a wireless network is the maintaining of Confidentiality, Authentication, and Non-repudiation and Integrity control [3]. We noticed that the security mechanism of IEEE 802.16 is mainly focusing on security in MAC sub-layer. This security sub layer in WiMAX network is where authentication, authorization and encryption take place [4]. To exchange data onto higher protection between MAC and PHY layer WiMAX defines a security sub- layer on the ground of MAC-layer. The security sub-layer contains the key management of protection keys, like AK (Authorization Key), TEK (Traffic Encryption Key), KEK (Key Encryption Key), or HMAC (Message Authentication Key) [5]. It also maintains privacy by ensuring that no eavesdropper can hijack the message between SS (Subscribe Station) and BS (Base Station).

For the encryption we use an algorithm at the MAC layer. The existing model uses the RSA algorithm; though we have opted to use ECC (Elliptic Curve Cryptography) based CA (Cellular Automata) in our proposed model.

II. LITERATURE SURVEY

Masood Habib et al. (2009) described WiMAX along with its security concerns in the paper. Some wireless protocols and encryption technique were studied and enhancements were proposed. It also found out that ECC is better than RSA is having smaller size 163 bits to 1024 bits and the delay was also smaller. It was also observed that WTLS certificate requires less memory than X.509 certificate [6].

Prakash Kuppuswany et al. (2014) had discussed about the use of new algorithm based on a block cipher for the replacement of RSA and to ensure the confidentiality, integrity and authentication. The Proposed algorithm used smaller key size linear block cipher is not to produce same key size as compared to RSA. The best benefit of linear block cipher is not to produce the same kind of result of repeated text variables. The authors had constructed 2 blocks, 3 block square matrix [7].

Rakesh Kumar Jha and Upena D Dalal (2010) had done different evaluations of WiMAX system and also shown the current capability and future trends in the WiMAX technology. It also deals with different threat applied to both layers of WiMAX at PHY as well MAC layer. The most common attacks are DOS attack. The authors said that if the security issues in fixed, then WiMAX could be successful wireless communication technology in the future [2].

M Alzaabi et al. (2013) found the various attacks on WiMAX and tried to find the solution to these various attacks. They identify DOS as one of the security threats which degrades the quality of service of WiMAX. The authors had given one of the best ways the blowfish algorithm to secure the management messages [4].

Daniel Simion et al. (2012) identified significant threats involved in the infrastructure of IEEE 802.16 (WIMAX Technology).This paper helps researchers to understand the vulnerability and the security in WiMAX. In this paper, the authors described that WIMAX technology has complex authentication and authorization method. But, still it is vulnerable on different attacks or threats. It will require a very special attention on security improvement [5].

Jamshed Hasan (2006) had brought up the changes by 802.16e like generating each per frame IV (initialization vector) randomly. The used of AES (Advanced Encryption standard) as main encryption method and introduced a flexible authentication method based on Extensible Authentication protocol, for example, EAP-TLS, EAP-TTLS, PEAP, EAP-SIM is extending the authentication to the server. The standard also replaces Triple-DES key wrapping in the PKM protocol with the AES-ECB mode [8].

V.P.Narkhede et al. (2015) proposed for implementing public key cryptosystem using Public key and private key; and some mathematical relation by RSA algorithm. RSA is limited by its larger computational requirements. This paper tells us RSA is one of the first practical public key cryptosystem and it is widely used for secure data transmission. In this Paper the security of RSA is still facing many problems and vulnerable to many threats [9].

Abdul Maalik et al. (2013) had revealed two objectives for WiMAX security, first to improve privacy over wireless link and second obligation is delivering access control effectively to the network. The authors used OMNET++ simulator [10].

Monika Rani et al. (2011) pointed out the vulnerabilities of 802.16 and threats to malicious attacks are raised. The security improvement is done using RSA algorithm. The proposed protocol is secure against both active and passive attacks. It is also efficient in saving the computational complexities [11].

Nentawe Y. Goshwe (2013) highlighted the need for security in data sharing over a network. The design of data encryption and decryption in a network environment using the RSA algorithm with a specific message block size is presented even if an eavesdropper comes between a sender and receiver, it will return a meaningless message [12].

Pranita K. Gandhewar and Kapil N. Hande (2011) had introduced new security measures of IEEE 802.16 which use Elliptic Curve Cryptography (ECC) encryption algorithm. This model of IEEE provides more security by protecting the network against unauthorized access. This paper shows ECC use smaller key size as compared to RSA [13].

III. PROPOSED WORK

A. Working on WiMAX Security Model

The proposed security model is depicted in Figure1. When MS needs to interface with the BS, then MS sends an authentication information messages (Authentication info MSG) which contains merchant endorsements of the MS serving BS to look at the reliability of the MS. As soon as BS receives authentication information messages, MS replies authentication request messages (Authorization Req MSG) to the BS which contains:

- MS certificate
- SAID
- Security capabilities.

On the off chance that the endorsement is not legitimate, then authorization rejected and on the off chance that it is lawful the BS generates AK and sends an authorization reply message which includes:

- AK encryption with EC^3A public key of MS
- 4-bit sequence number
- Lifetime of AK
- WTLS certificate of BS

The proposed security model utilizes EC^3A algorithm for encryption and decryption. Subsequently BS also calculates the KEK and HMAC(for downlink & uplink) key. As MS gets an authentication reply message, it attests the BS certificate. If it is legal it extracts the AK from the message and calculates the KEK and HMAC key.

The following stride sends the TEK request (TEK Req) to the BS which incorporates:

- SAID
- AK sequence number
- HMAC digest

BS first validates the HMAC digest. If it's valid, then BS generates the TEK and sends the TEK which contains:

- SAID
- AK sequence number
- TEK
- TEK lifetime
- HMAC digest

When key exchange phase is done successfully, BS is encrypted with the TEK excluding header and CRC checksum.

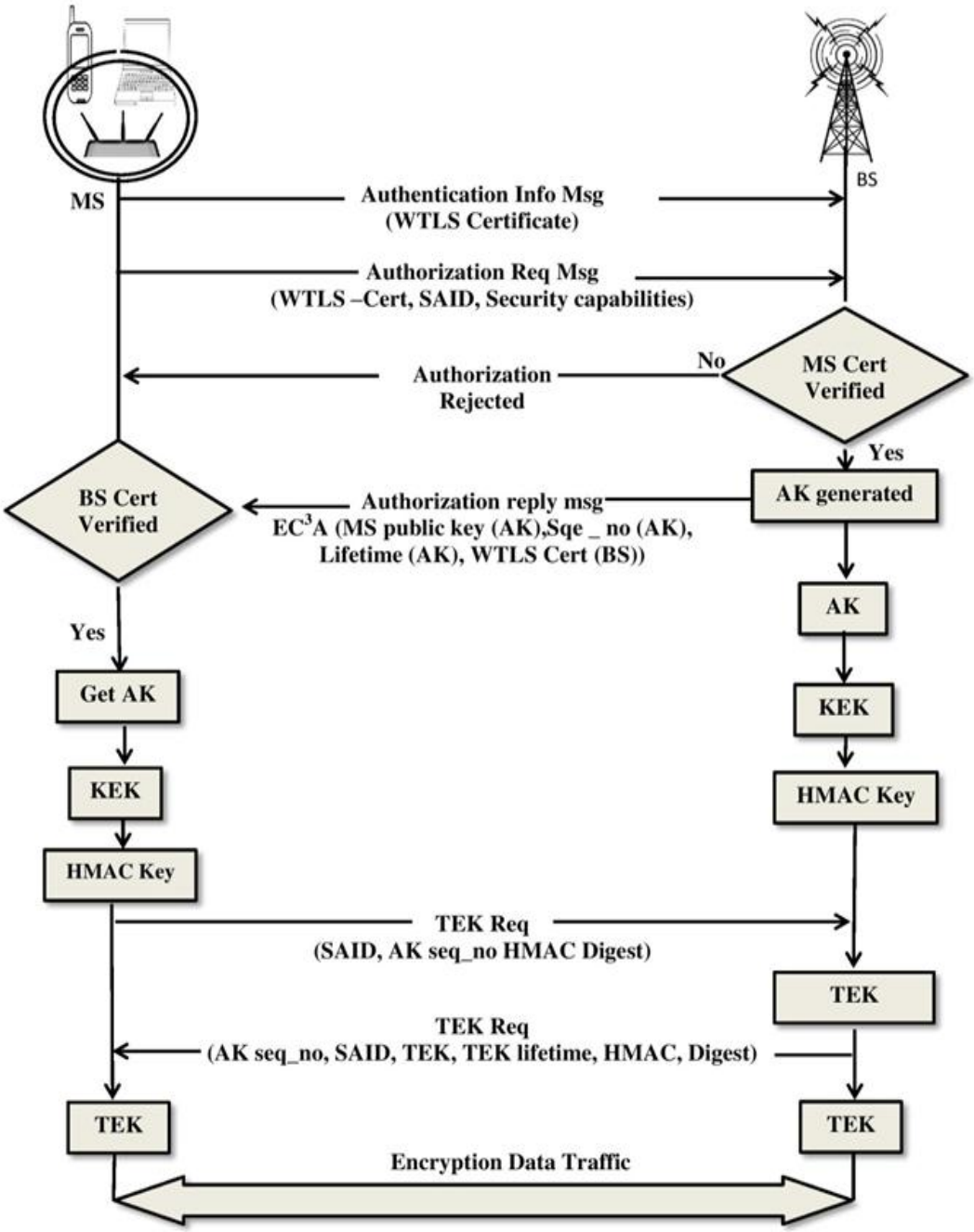

Fig-1 Proposed WiMAX Security Model

B. Elliptic Curve Cryptography based on cellular automata (EC3A)

Elliptic Curve Cryptography is a way to deal with public-key cryptography in light of the algebraic structure of elliptic bends over finite fields. ECC requires littler keys contrasted with non-ECC cryptography (in view of plain Galois fields) to give equal security.

An elliptic curve is pertinent for encryption, digital signatures, and pseudo-arbitrary generators. They are likewise utilized as a part of a few number factorization algorithm in view of elliptic curve which have applications in cryptography, for example, Lenstra elliptic curve factorization.

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography.

Cellular Automata (CA) are a discrete computing model which provides simple, flexible and efficient platform for simulating complicated systems and performing complex computation based on the neighbourhood information. CA consists two components: 1) a set of cells and 2) a set of rules. Researchers, scientists and practitioners from different fields have exploited the CA paradigm for modelling different applications.

A cellular automaton consists a graph where each node acts as a cell. The state of each cell is updated simultaneously at discrete time steps, based on the states in its neighbourhood at the preceding time step. The algorithm used to compute the next cell state is referred to as the CA local rule.

Flow chart of the EC^3A encryption and decryption algorithm is depicted in figure 2 and figure 3.

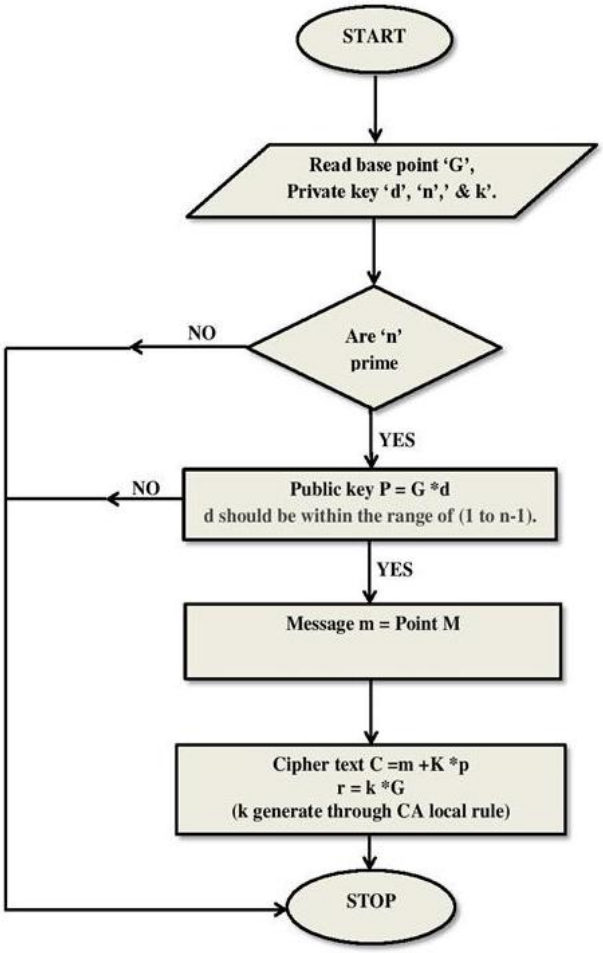

Fig .2: Flow Chart of the EC^{3}A Encryption Algorithm

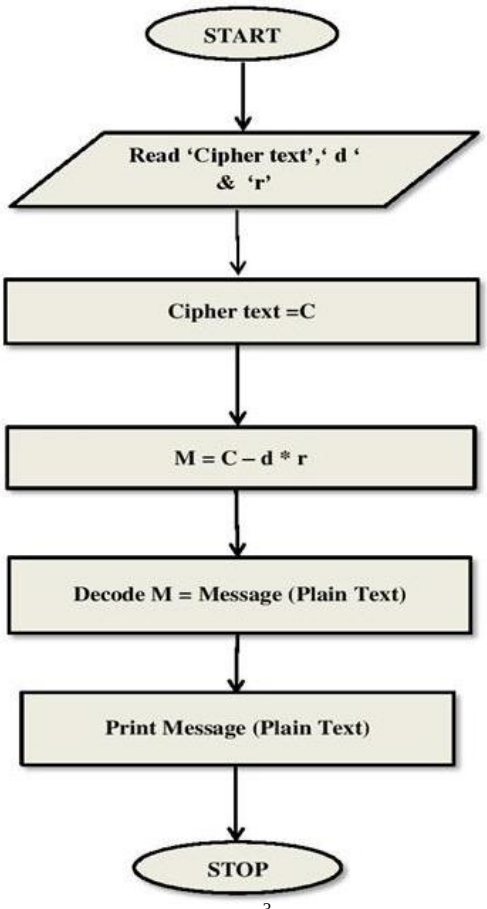

Fig. 3: Flow Chart of the EC^{3}A decryption Algorithm

C. Mathematical Simulation of EC3A

The equation of an elliptic curve is determined as: $y^3 = x^3 + ax + b$.

Let the elliptic curve $y^2 \bmod 13 = (x^3 + x + 6) \bmod 13$ and Now we determine y when x = 2,

$y^2 \bmod 13 = (8 + 2 + 6) \bmod 13 = 3 \Longrightarrow y = \pm 4 \bmod 13 = 4$ and 9.

We get two points P (2, 4) and - P = (2, 9) on the elliptic curve. These points are inverse to each other. We can determine other points of $E_{13}(1, 6)$ in a similar manner .Table 1 shown all the points of set $E_{13}(1, 6)$.The values of y^2 for x = 0, 1, 5, 7, 8, and 9 do not have square root modulus 13. We do not have points in $E_{13}(1, 6)$ corresponding these values 0.

Table I Elements of $E_{13}(1, 6)$

X	y^2(mod11)	Y	P	–P
2	3	4, 9	(2, 4)	(2, 9)
3	10	6, 7	(3, 6)	(3, 7)
4	9	3, 10	(4, 3)	(4, 10)
9	1	4, 9	(9, 4)	(9, 9)
11	9	3, 10	(11, 3)	(11, 10)
12	12	2, 11	(12,2)	(12, 11)
–	–	–	0	0

***Case 1*:** If we consider the point G = (2, 9) lies on the elliptic curve $y^2 \bmod 13 = (x^3 + x + 6) \bmod 13$, determine 2G, 3G, 4G, 5G, 6G and so on.

$x_{2P} = \left[\frac{3x_P^2 + a}{2y_P}\right]^2 - 2x_P$ and $y_{2P} = \left[\frac{3x_P^2 + a}{2y_P}\right]^2 (x_P - x_{2P}) - y_P$ (For doubling point)

$$x_{2G} = \left[\left[\frac{3 \times 2^2 + 1}{2 \times 9}\right]^2 - 2 \times 2\right] \bmod 13 = \left[\frac{169}{324} - 4\right] \bmod 13 = [0 - 4] \bmod 13$$

$x_{2G} = -4 \bmod 13 = 9$

$$y_{2G} = \left[\left[\frac{3 \times 2^2 + 1}{2 \times 9}\right] \times (2 - 9) - 9\right] \bmod 13 = \left[\frac{13}{18}(-7) - 9\right] \bmod 13$$

$y_{2G} = [0 - 9] \bmod 13 = 4$.

We got $x_{2G} = 9$ and $y_{2G} = 4$ therefore 2G = (9, 4). Similarly, we had computed 3G, 4G, 5G, & so on.

Table III Group E_{13} with the Generator G = (2, 9)

G=(2,9)	5G=(3,6)	9G=(12,11)	13G=(0)
2G=(9,4)	6G=(4,10)	10G=(11,10)	
3G=(11,3)	7G=(4,3)	11G=(9,9)	
4G=(12,2)	8G=(3,7)	12G=(2,4)	

Key Generation: Private and Public key generation consists of the following steps:

1. Sam chooses the base point $G_s = (2, 9)$ in $E_{13}(1, 6)$.
2. Private key $d_s = 7$
3. Compute public key $P_S = d_s * G_s$. $P_S = 7(2, 9) = 7\ G_s = (4, 3)$. $P_S = (4, 3)$

Sam announces $\{E_x(a,b), G_s, P_S$ ie. $E_X (1, 6), G_s = (2, 9)\ P_S = (4,3)\}$.

Encryption: Cipher text $C = m + k * P_S$

Where k is random number chooses through Cellular Automata and m is the message.

$r = k * G_s$ and m = (9, 9) and k =9. Now put the value m and k in above equation.

$C = m + k.\ P_S \Longrightarrow C = (9, 9) + 9(4, 3) \Longrightarrow C = 11G + 9.7G = 11G + 63G = 74G$

$C = 13G + 13G + 13G + 13G + 13G + 9G \Longrightarrow C = 9G = (12, 11)$.

$r = k * G_s = 9(2, 9) = 9G = (12, 11)$.

Decryption: Plaintext (P) = C – $d_s * r$. We can expand the equation of the plain text.

Plaintext (P) = m + (k. * P_S) – (d_s *k*G_s.).Now put the value of C, ds and r and get the Plain text (P).

P= 9G – 7*9* G ⟹ P = 9G – 63 G ⟹ P = 54G = – {13G + 13G + 13G +13G +2G}

P = – {0 +2G} ⟹ P = – (2G) = – (9, 4) ⟹ – (9, 4) = (9, 9) since 2G + 11G =0.

Key Exchange using Elliptic Curve Cryptography Based on Cellular Automata:

1. Sam and Ria choose elliptic curve E_x (a, b) and base point G on the curve.Such that E_x(1,6) and base point G (2,9).
2. Sam selects a secret integer cellular automata $n_s < N$, being the order of G. Sam generates point $P_S = n_sG$ on the elliptic curve. Sam sends P_S and n to Ria.
   $n_s < N$, where n is Sam select her secret integer (n=5)and N is order (N= 13).
   5 < 13, $P_S = n_sG$. P_S = 5G = (3, 6).
3. Ria selects a secret integer $n_R < N$, and generates point $P_R = n_RG$ in similar way, Ria sends P_R to Sam.
   $N_R < N$ ⟹ 11< 13 where we taking n_R value is 11.$P_R = n_RG$ ⟹ P_R = 11G ⟹ P_R = (9, 9).
4. Sam and Ria calculate a shared secret could subsequently be used as symmetric- key as fallows.
   - Sam calculates the shared secret key k as

   k = n_s P_R = 5(9,9) ⟹ k = 5 * 11G ⟹ K = 55G. k = 13G + 13G +13G +13G + 3G ⟹ k = 0 + 3G.
   k = 3G ⟹ k = 3G ⟹ k = (11, 3).
   - Ria calculates the shared secret key K as

   k = n_R P_S = 11(3, 6) ⟹ k = 11 * 5G ⟹ k = 55G. k = 13G + 13G +13G +13G + 3G ⟹ k = 0 + 3G.
   k = 3G ⟹ k = 3G ⟹ k = (11, 3).
   So we can say that k = n_s P_R = n_R P_S.

Case 2: If we consider the point G = (4, 3) lies on the elliptic curve y^2 mod 13 = (x^3 + x + 6) mod 13, determine 2G, 3G, 4G, 5G, 6G and so on.

$$x_{2G} = \left[\left[\frac{3 \times 4^2 + 1}{2 \times 3}\right]^2 - 2 \times 4\right] \bmod 13 = \left[\frac{2401}{36} - 8\right] \bmod 13 = [10 - 8] \bmod 13$$

x_{2G} = 2 mod 13 = 2.

$$y_{2G} = \left[\left[\frac{3 \times 4^2 + 1}{2 \times 3}\right] \times (4 - 2) - 3\right] \bmod 13 = \left[\frac{49}{6}(2) - 3\right] \bmod 13$$

$$y_{2G} = [12 - 3] \bmod 13 = 9.$$

We got 2G = (2, 9). Similarly we had computed 3G, 4G, 5G and so on.

Table III Group E_{13} with the Generator G = (4, 3)

G=(4,3)	5G=(12,11)	9G=(9,9)	13G=(0)
2G=(2,9)	6G=(11,3)	10G=(3,6)	
3G=(3,7)	7G=(11,10)	11G=(2,4)	
4G=(9,4)	8G=(12,2)	12G=(4,10)	

Case III : If we consider the point G = (11, 10) lies on the elliptic curve y^2 mod 13 = (x^3 + x + 6) mod 13, determine 2G, 3G, 4G, 5G, 6G and so on.

$$x_{2G} = \left[\left[\frac{3 \times 11^2 + 1}{2 \times 10}\right]^2 - 2 \times 11\right] \bmod 13 = \left[\left[\frac{364}{20}\right]^2 - 2\,2\right] \bmod 13$$

$$x_{2G} = \left[\frac{8281}{25} - 22\right] \bmod 13 = [0 - 22] \bmod 13 = 2 \bmod 13 = 4.$$

$$y_{2G} = \left[\left[\frac{3 \times 11^2 + 1}{2 \times 10}\right] \times (11 - 4) - 10\right] \bmod 13 = \left[\frac{364}{20}(7) - 10\right] \bmod 13$$

$$y_{2G} = [0 - 10] \bmod 13 = 3.$$

We got 2G = (4, 3) similarly we had computed 3G, 4G, 5G, and so on.

Table IV Group E_{13} with the Generator G = (11, 10)

G=(11,10)	5G=(9,9)	9G=(2,4)	13G=(0)
2G=(4,3)	6G=(3,7)	10G=(12,11)	
3G=(12,2)	7G=(3,6)	11G=(4,10)	
4G=(2,9)	8G=(9,4)	12G=(11,3)	

D. Comparison of ECC with RSA algorithm

Elliptic Curve Cryptography is better than RSA for many purposes. The key size of ECC less than RSA (key size ECC -512 ~ RSA-15424). ECC more secure and robust than RSA. To improve the security level, we incorporated CA in Elliptic Curve Cryptosystems.

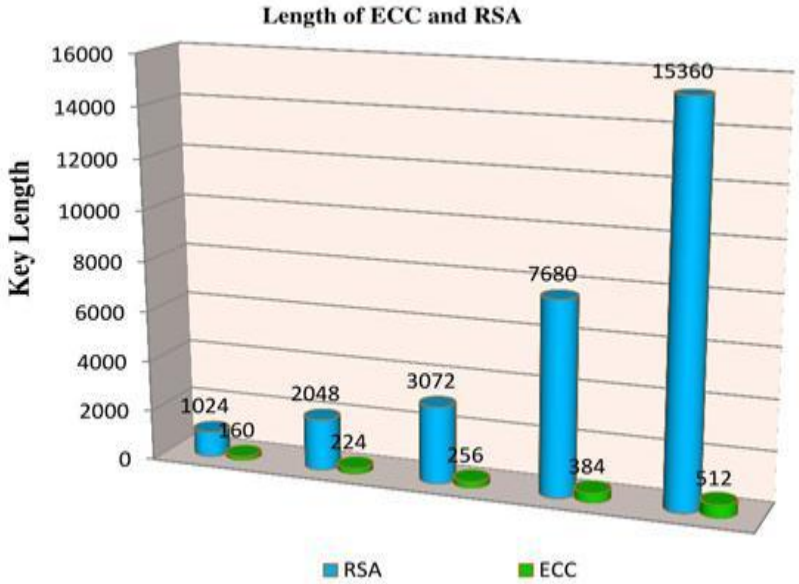

Fig-4 Key Size of RSA and ECC

IV. CONCLUSION

In this paper, we have improved to the current model to expand its abilities and security. We came up with two enhancements; 1. Used the ECC with cellular automata (CA) than RSA 2. WTLS certificate use the minimum memory storage than X.509 certificate. We introduced the concept of Cellular Automata (CA) as a promising approach to enhance the security of ECC. Though, our proposed protocol is the potential solution for WiMAX security. In fact, Cellular Automata are the strengthen method to generate strong keys. In future, Cellular Automata (CA) can be combined with several public key cryptography algorithms to get efficient results.

REFERENCES

[1] http:// en. Wikipedia.org/wiki/WiMAX. Last accessed on Jan 2017.

[2] Rakesh Kumar Jha, and Upena D Dalal, "A journey on WiMAX and its security issues," International Journal of Computer Science and Information Technologies(IJCSIT), Vol. 1 (4) , pp. 256-263, 2010.

[3] Sanjay P. Ahuja, Nicole Collier, "An Assessment of WiMAX Security," Communication and Network, Vol.2, pp. 134-137,May 2010.

[4] M Alzaabi, K D Ranjeeth, T Alukaidey and K Salman, "Security algorithms for WiMAX," International Journal of Network Security & Its Applications (IJNSA), Vol.5, pp. 31-44, May 2013.

[5] Daniel Simion, Mihai-Florentin Ursuleanu,and Adrian Graur,"An overview on WiMAX security weaknesses/ potential solutions,"11th International Conference on Development and Application Syestem, Suceava, Romania, May 2012, pp.98-102.

[6] Masood Habib,Tahir Mehmood,Fasee Ullah,Muhammad Ibrahim, "Performance of WiMAX Security Algorithm," International Conference on Computer Technology and Development (ICCTD), 2009, pp.108-122.

[7] Prakash Kuppuswamy, Sikandhar Shah,"Improving security authentication of IEEE 802.16 WiMAX with new public key algorithm," International Journal of Engineering and Computer Science, Vol.3, pp.3965-3970, Feb. 2014.

[8] Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)," Symposia and Campus Event, Australian Information Security Management Conference (AISMC), 2006.

[9] V.P.Narkhede, P.S.Ajabe, and.S.M.Dandage, & P.B.Zope, "A review of public key cryptography for secure communication using RSA", International Journal of Advent Research in Computer and Electronics (IJARCE) (E-ISSN: 2348-5523) Special Issue, National Conference "Convergence", pp.1-4, March 2015.

[10] Abdul Maalik, Mamoona Naz and M. J. Qureshi, "Implementation of MAC Layer Security Protocol in WiMAX Using OMNET++ Simulator," International Journal of Computer Science and Telecommunications, Vol.4, pp.34-43, Aug. 2013.

[11] Monika Rani, Anil Rose and Mridul Chawla, "Review of public key cryptography on WiMAX using RSA algorithm," Journal of Engineering Research and Studies (JERS), Vol. 2, pp.219-222, October-December, 2011.

[12] Nentawe Y. Goshwe, "Data encryption and decryption using RSA algorithm in a network environment," International Journal of Computer Security (IJCSNS), Vol. 13, pp. 9-13, July 2013.

[13] Pranita K. Gandhewar, & Kapil N. Hande ,"Performance improvement of IEEE 802.16 / WiMAX using elliptic curve cryptography," International Journal of Computer Science and Information Technologies, Vol. 2, pp. 1309-1311, 2011.

