ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.6, 3295–3306
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.6.9 Spec. Issue on RDESTM-2020

# ENHANCED ELLIPTIC CURVE CRYPTOGRAPHY BASED SECURE ROUTING IN LTE NETWORK

KRISHAN KUMAR[1] AND YOGESH CHABA

ABSTRACT. Long Term Evolution is considered as an important innovation of current wireless communication systems. Long Term Evolution improves the limit and decreases the multifaceted nature of system availability, and furthermore empowers administrators to limit their operational expenses. In this technology, eNodeB is used to refer to a typical base station. In any case, clients in this technology are confronting a few difficulties those are to be explained. Routing and security are the issues which happen during the information transmission. On the off chance if client is not in range with the base station and still needs to speak with the base station, the correspondence must be secured. To accomplish this necessity, Oppositional Particle Swarm Optimization based Enhanced Elliptic Curve Cryptography (EECC) is exhibited in this research. It is notable that elliptic curve cryptosystem based algorithm would be best decision because of their small key sizes and proficient calculations. The existing algorithm is upgraded or optimized by utilizing Oppositional Particle Swarm Optimization algorithm and further it is utilized to produce the ideal key qualities. In light of the optimal key value data is safely conveyed to the eNB. The proposed algorithm is actualized in the stage of Network test system NS3. The exhibition of the proposed methodology is assessed far parameters such as delivery ratio and delay which shows considerable improvement.

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A60, 14G50.

*Key words and phrases.* LTE, Communication, Security, Routing, EECC, OPSO.

## 1. INTRODUCTION

Wireless network administrators today commit extensive manual exertion in arranging, designing, upgrading and keeping up their remote access systems. These endeavors have an incredible stake in their operational uses. The institutionalization body third Generation Partnership Project (3GPP) has designed the technology Long Term Evolution(LTE) [1]. Long haul Evolution speaks to a developing innovation that guarantees a broadband and universal Internet get to. In any case, a few angles must be considered for giving viable sight and sound administrations to portable clients. Plainly the streamlining of all LTE perspectives is a subject worth of examination for industry and the scholarly world networks, especially considering mixed media applications. Other than higher piece rate, lower inertness and numerous other administration contributions for LTE, user equipment (UE) control sparing is a significant issue [2]. LTE system is a low defer, all IP and high throughput technology. So as to diminish start to finish delay, the quantity of system hubs is diminished in the standard of LTE. One of the effective characteristics of the LTE system is low start to finish postponement [3]. LTE framework, called now and again super 3G, is required to offer a phantom proficiency between 2 to multiple times greater than 3GPP. One of the open key cryptosystems is Elliptic curve cryptography [ECC]. An open key and a private key are owned by every client. To confirm encryption/signature, open key is used. For decoding/signature age private key is used. Elliptic bends are utilized as an augmentation to other current cryptosystems [4]. With the blast of systems and the gigantic measure of information transmitted along, verifying information substance is ending up increasingly significant. Encryption of information is broadly utilized in open systems, like the Internet for guaranteeing security. The cryptosystem dependent on Elliptic Curve Cryptography is turning into the ongoing pattern of open key cryptography [5]. Further, there are incredibly proficient, conservative equipment executions are accessible for ECC exponentiation tasks, offering potential decreases in usage impression even past those because of the littler key length alone. ECC isn't just risen as an alluring open key crypto-framework for versatile/remote conditions, yet in addition, provides data transfer capacity investment funds [6]. Various techniques have been developed over the years to overcome problems in routing mechanism of Long Term Evolution in any network out of which some are described in the

next section. In this paper an Enhanced Elliptic Curve Cryptography technique for LTE is presented. Introduction about LTE Technology is given in Section 1. Related work is discussed in Section 2. Enhanced Elliptic Curve Cryptography using OPSO is presented in Section 3. Performance and results of proposed method is evaluated in Section 4. Conclusion is given in Section 5.

## 2. PRELIMINARIES

Many techniques have been proposed in literature for improving the performance of LTE network. Elliptic bend based cryptosystem displays its capacity and is appropriate for the cutting edge open key cryptosystem. ECC offers a superior execution since it can accomplish a similar security with a littler key size. In 2010 Ritu *et al.* proposed an IPC key management scheme for wireless sensor network for providing improved security in network [7]. Lai *et al.*[8] in 2013 proposed a protected and proficient AKA convention SE-AKA to fit in the LTE systems with the majority of the gathering verification situations. Contrasted and other verification conventions, SE-AKA can't just give solid security properties including protection safeguarding and KFS/KBS, yet additionally give a gathering confirmation instrument which can viably validate bunch gadgets. Further is 2015 Balamurugan *et al.* [9] have introduced a faster mapping system in which the alphabets in the message were matched with dots in an elliptical curve. Then by using ElGamal encryption method, these points were encrypted utilizing a non-single-matrix matrix. By decrypting the encoded message utilizing the ElGamal decryption method, and by multiplying the decoded matrix by the inverse of the single non-matrix, the original message is obtained. To establish a secure connection and to encrypt the data, Tirtani *et al.* [10] in 2014 have demonstrated linear cryptography and ECC respectively. A four step process has been presented with the assistance of the demonstrated methods to guarantee the user's credibility. The initial step is connection establishment, second step is creation of an account, third step is authentication and the final step is data transfer. As the ECC algorithm's speed is high and the computational cost is lower than the other linear algorithms, ECC has been utilized. For achieving data security in D2D communications, a new secure data sharing protocol has been presented by Zhang *et al.* [11] in 2015 by combining the benefits of symmetric encryption and public key cryptography. In particular, the

public key-based digital signature merged with the cellular network's mutual authentication mechanism ensures the transmission non-repudiation, entity authentication, detectability, data authority and integrity. For guaranteeing data confidentiality symmetric encryption was utilized. For secure handover session key management through mobile relay on networks of LTE-A, Qinglei Kong *et al.* [12] in 2016 presented a scheme in which approach was utilized to achieve forward and backward key separation, a shared session key between the on-board UE and the connected donor evolved Node B (DeNB), which is first created by the on-board UE and then securely distributed to the DeNB. Long-term Evolution-Advanced (LTE-A) and Long-term Evolution (LTE) networks support highly developed encryption and authentication mechanisms. However, these systems are still plagued by replay attacks, impersonation attacks, known key attacks, eavesdropping attacks and many other security issues. Louw *et al.* in 2016 proposed a protocol of key conveyance that was meant to safely provide verified bits mystery framework keys utilizing cryptographic capacities based on ECC. The planned plan satisfied the basic necessities for a plan of key circulation to be viewed as protective and effective in WSNs [13].To alleviate these security weaknesses, Prabhat Panda and Chattopadhyay [14] in 2019 have introduced an enhanced authentication and security plan for the networks of LTE / LTE-A networks. The approach uses salsa20, elliptical curve cryptography (ECC) and Elliptic curve Diffie-Hellman (ECDH) algorithms. That scheme uses many powerful encryption approaches and also proper mutual authentication is provided among the Message Management Agency (MME) and the User Equipment (UE). The proposed system's performance is compared to the existing and LTE-A systems in terms of many performance parameters and security attributes.

In review of literature, many methods/algorithms have been proposed for improving the performance of Long Term Evolution from routing and security point of view. One of the primary difficulties of LTE is to accomplish high unearthly effectiveness, which means the utilization of the entire of the framework's transfer speed in all cells. Client hardware (UE) control sparing is another significant issue.Improving the presentation of the framework without giving up its security by utilizing a diminished quantity of ECC point duplication can be viewed as a significant testing issue. During handover, a huge computational overhead and a long postponement may happen. In this paper these problems have been

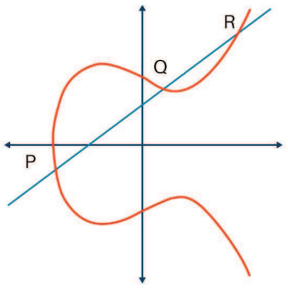


FIGURE 1. Elliptic Curve Cryptography

addressed and solution has been proposed for improving the performance by enhancement of existing techniques.

## 3. ENHANCED ECC BASED SECURE ROUTING IN LTE

In this work, Enhanced Elliptic Curve Cryptography (EECC) is presented for secured routing in LTE network. The ECC algorithm is enhanced or optimized by using Oppositional Particle Swarm Optimization (OPSO) algorithm. This algorithm is used to generate the optimal key values.Based on the key values data is transmitted to the eNB. Multiple data is transmitted between User Equipment and eNodeB using Enhanced Elliptic Curve Cryptography. Then this algorithm generates optimal values using OPSO algorithm and then data is routed securely.Elliptic Curve Cryptography (ECC) an open key cryptography is improved. The ECC approach has the potential to generate public keys and private keys, which make distributed information more protective. The general equation for ECC and graphical representation (figure 1) of ECC is given below:

$$p^2 = q^2 + \delta q + \Delta$$

The key age procedure is utilized to produce the open key and private key. Key is generated by a process in which, the sender encodes the data with the assistance of recipient's open key and collector unscrambles the data utilizing private key. After key generation process encryption and decryption takes place.

3.1. **Algorithm for Proposed OPSO based ECC.** ECC is optimized or enhanced by using Oppositional Particle Swarm Optimization (OPSO) calculation. This algorithm is used to make the ideal key characteristics. As the amount of transmissions is occurred through the different ways, data pace of the framework's rate of data is upgraded. Regardless, some routing ways may lose its security and besides they are presented to block of between ways. In this way, to vanquish these issues, an deal key to be looked over the amount of keys. For optimal key selection, OPSO is utilized. Detailed steps in proposed algorithm are as follows:

*Initialization:* The presented approach to manage instatement of population uses the obstruction based technique in which the inputs are population and its contrary populace. This technique's candidate solution is ideal key between source UE and eNB. The solutions' initialization can be indicated as,

$$P_{N_m} = P_{n_1} + P_{n_2} + P_{n_3}.....P_{n_i}$$

Where, the prime numbers of $n^{th}$ population is denoted by $P_{N_n}$. Number of dimensions is denoted by $d$. Here, $i = 1, 2, 3...d$

*Fitness calculation:* After the initialization of swarms or ideal key, the particle swarm's fitness is assessed. It is characterized as the capacity that estimates optimality of a solution and commonly it is the objective function. The fitness limit is described reliant on the throughput of the solution in this technique for ideal key or private key selection. The extent between the size of the plaintext and the encryption times is described as the throughput of the solution. It is dictated by using the following condition,

$$Thr_n = \frac{SizeofPlainText}{EncryptionTime}$$

$Thr_n$ represents the throughput of $n^{th}$ solution. SolutionâĂŹs Fitness function is evaluated as,

$$Fitness = Max\{thr_n\}$$

Each particle in the swarm deals with three qualities of d-dimensions.

*Local best (l-best)*: It is the best position where a particle has been getting the most noteworthy estimation of readiness for that particle. This value can be littlest for a smaller task.

*Global best (g-best)*: It is the position where the best fitness is cultivated by any particle of the swarm created up until this point.

*Update function*: After computing the fitness to the position of the swarm, it will be updated to the following position. Relying upon the altered exhibitions, such as global best and local best, the particle swarm is updated to next position. These exhibitions are portrayed as follows:

*Velocity Update*: Velocity is a d-dimensional vector that dictates the advancement velocity and particle's direction. By the going with condition given beneath, the velocity is updated.

$$V_{i+1} = wV_i + C_1 rand(0,1)K_{lbest} - K_i + C_2 rand(0,1)K_i\,.$$

Here, the inertia weight is denoted as $w$, the constant coefficients are denoted by $C_1$ and $C_2$; the local and global bests of the keys are denoted by $K_{lbest}$ and $K_{gbest}$ respectively.

*Position Update*: Each particle updates its position to move in the direction of solution in search of ideal solution. All of the particles in a swarm moves stochastically for ideal positions and update their positions using the following condition,

$$K_{i+1} = k_1 + V_i\,.$$

After getting the g-best and l-best of swarm, fitness of swarm will be calculated. If the g and l-best is satisfies the fitness, then the optimal solution is attained. Otherwise, the g-best and l-best will be updated using velocity and position. Finally, the source UE forwards the data securely to the eNB on the selected optimal key Opkn. The fig.4 shows the flow chart of OPSO.Subsequent to getting the swarm's g-best and l-best, swarm's fitness will be determined. In the event that the g and l-best is fulfills the fitness, at that point the ideal solution is achieved. Or else, the g-best and l-best will be updated utilizing position and velocity. At last, the source UE advances the information safely to the eNB on the chosen ideal key $O_{p_{k_n}}$.

3.2. **Algorithm of Oppositional Particle Swarm Optimization (OPSO).** Algorithm which implements steps given in previous section is as given below:
Input: Prime numbers

$$P_{N_m} = P_{n_1} + P_{n_2} + P_{n_3}.....P_{n_i}$$

Output: Optimal key values

- Initialize swarm of particles $P_{N_n}$ randomly, with $N$ as population size.

TABLE 1. Simulation Parameters

| Parameters | Values |
|---|---|
| eNB coverage radius | 375mt |
| System Bandwidth | 10MHz |
| Transmit Power | 43dBm |
| Receiver Sensitivity | -110 dBm |
| Number of UEs | 30 |
| Area | 1000x1000m |
| eNBs Distance | 400m |
| Routing protocol | AOMDV |
| Simulation time | 100s |

- Evaluate opposition of swarm *opposition of* $P_{N_n}$ using 3
- Evaluate the fitness of population based on the fitness function *Fitness* = *Max* $\{thr_n\}$
- Choose $N$ fittest individuals from set *opposition of* $P_{N_n}$,$P_{N_n}$ as initial population depending on fitness value
- Repeat
  - Calculate g-best
  - Repeat for every particle $P_{N_n}$
    - Calculate $P_{best}$
    - Update velocity and position components using 3.1 and 3.1 respectively
- Until <termination condition>

## 4. RESULTS AND DISCUSSION

Proposed OPSO based ECC is executed in the Network Simulator-3 (NS3). In this scenario, 30 UEs are exhibited and are moving in 1000x1000m reproduction region. Two eNBs are available with radius of 375m. These two eNBs are 400m away from each other. Transmit intensity of every terminal in the system is 43dBm. For bundle streeming, AOMDV directing convention is used. With these parameters, the modified code is executed for 100 seconds. Table 1 demonstrates the simulation parameters and values.

The proposed approach of OPSO based ECC is evaluated by finding out the

TABLE 2. Evaluated values of Delivery Ratio in Modified ECC using OPSO

| **Delivery Ratio in %age** | | |
|---|---|---|
| No. of Active Users | ECC | Modified ECC using OPSO |
| 10 | 0.60 | 0.97 |
| 15 | 0.57 | 0.92 |
| 20 | 0.48 | 0.85 |
| 25 | 0.42 | 0.73 |
| 30 | 0.38 | 0.70 |

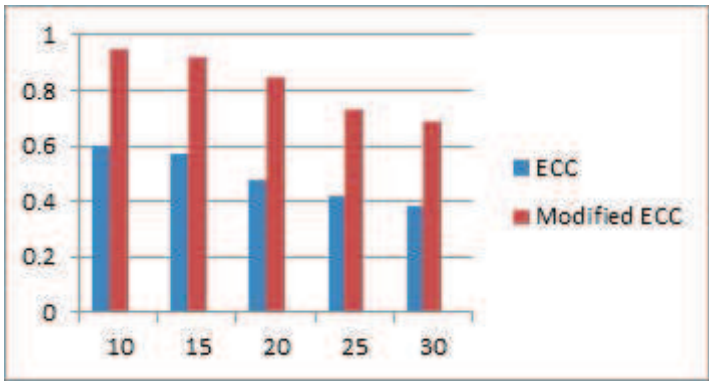


FIGURE 2. Bar Chart for Evaluated values of Delivery Ratio in Modified ECC using OPSO

delay and packet delivery ratio for various numbers of users such as 10, 15, 20, 25 and 30. These results are compared with that of existing method ECC.

4.1. **Delivery Ratio.** It is the proportion of the quantity of packets received and the aggregate sum of packets transmitted

$$D.r = \frac{No.of PacketsReceived}{No.Of PacketsTransmitted}.$$

Table 2 and corresponding Figure 2 demonstrates the comparison of delivery ratio of OPSO-ECC with the current method ECC for various numbers of users. Contrasted with ECC, conveyance proportion of the proposed OPSO-ECC starts from 70% when number of actives nodes are 30 and most extreme conveyance proportion of our proposed technique is 97% as compared to existing ECC which is 60 % maximum and 38% minimum

TABLE 3. Evaluated values of Delay in Modified ECC using OPSO

| Delay in mSec | | |
|---|---|---|
| No. of Active Users | ECC | Modified ECC using OPSO |
| 10 | 690 | 265 |
| 15 | 820 | 220 |
| 20 | 805 | 400 |
| 25 | 980 | 490 |
| 30 | 1000 | 575 |

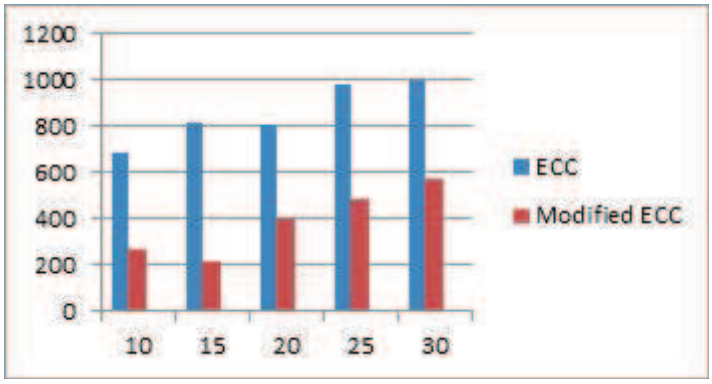


FIGURE 3. Bar Chart for Evaluated values of Delay in Modified ECC using OPSO

4.2. **End to End delay:** The delay of system indicates to what extent the system takes to transmit a bit to the destination. The Unit of this parameter is in milliseconds (ms).

Table 3 and corresponding Figure 3 demonstrates the comparison of delay of OPSO-ECC with the current method, ECC for various numbers of users. Contrasted with ECC, delay of the proposed OPSO-ECC is in the range of 265 mSec when number of actives nodes are 10 and maximum delay is 575 mSec when number of active users are 30 as compared to existing ECC which ranges from 690 mSec to 1000 mSec.

## 5. CONCLUSION

In this work, OPSO based ECC is proposed with the Extracts of the Elliptic Curve Cryptography (ECC), Diffe-Hellman key trade to improve the security

and routing. Along these lines, EECC is introduced in this work. It is prominent that elliptic curve cryptosystem (ECC) based calculation would be best choice as a result of their little key sizes. The ECC calculation is upgraded by using Oppositional Particle Swarm Optimization (OPSO) calculation and moreover the OPSO is used to deliver the perfect key characteristics. The proposed EECC is implemented in NS3 Network Simulator. Itemized assessments of execution represent that the proposed strategy accomplishes better execution as far as vitality, productivity, conveyance proportion and postponement contrasted then existing strategies. From the comparative diagrams, it is clear that the proposed EECC outperforms existing Elliptic Curve Cryptography technique in terms of Packet Delivery Ratio and Delay.

## REFERENCES

[1] S. L. CHRISTOPH, M. AMIRIJOO, A. EISENBLAETTER, R. LITJENS, M. NEULAND, J. TURK: *A coordination framework for self-organisation in LTE networks,* Proc 12th IFIP/IEEE International Symposium on Integrated Network Management, (2011), 193–200.

[2] C. FRANCESCO, G. PIRO, L. A. GRIECO, G. BOGGIA, P. CAMARDA: *Downlink packet scheduling in LTE cellular networks: Key design issues and a survey*, IEEE Communications Surveys and Tutorials, **15**(2) (2012), 678–700.

[3] S. VOLKAN, J. WANG, O. BAYAT, J. WEITZEN: *Cosine operator functions and Hilbert transformations*, Novi Sad J. Math., **35**(2) (2005), 41–55.

[4] G. VEERRAJU, S. INUGANTI, S. MUPPIDIZEN: *Data security in cloud computing with elliptic curve cryptography,* International Journal of Soft Computing and Engineering (IJSCE), **2**(3) (2012), 138–141.

[5] V. S. MARIA CELESTIN, K. MUNEESWARAN: *Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications,* IJ Network Security, **14**(4) (2012), 236-242.

[6] F. AMOUNAS, E.H. EL-KINANI: *An efficient elliptic curve cryptography protocol based on matrices,* International Journal of Engineering Inventions, **1**(9) 2012, 49–54.

[7] R. SHARMA, Y. CHABA, Y. SINGH: *An IPC key management scheme for wireless sensor network,* Proc. 1st International Conference on Parallel, Distributed and Grid Computing, 2010.

[8] L. CHENGZHE, H. LI, R. LU, X. S. SHEN: *SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks,* Computer Networks, **57**(17) (2013), 3492–3510.

[9] R. BALAMURUGAN, V. KAMALAKANNAN, D. GANTH, D. RAHUL, S. TAMILSELVAN: *Enhancing security in text messages using matrix based mapping and ElGamal method in*

*elliptic curve cryptography*, Proc. International Conference on Contemporary Computing and Informatics, (2014), 103–106.

[10] T. NEHA, R. GANESAN: *Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography*, IACR Cryptology ePrint Archive **49** (2014).

[11] Z. AIQING, J. CHEN, R. QINGYANG HU, Y. QIAN: *SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks,* IEEE Transactions on Vehicular Technology, **65**(9)(4) (2015) 2659–2672.

[12] K. QINGLEI, R. LU, S. CHEN, H. ZHU: *Achieve secure handover session key management via mobile relay in LTE-advanced networks*, IEEE Internet of Things Journal, **4**(1) (2016), 29–39.

[13] J. LOUW, G. NIEZEN, T. D. RAMOTSOELA, A. M. ABU-MAHFOUZ: *A key distribution scheme using elliptic curve cryptography in wireless sensor networks*, Proc. 14th International Conference on Industrial Informatics (2016), 1166–1170.

[14] PANDA, P. KUMAR, S. CHATTOPADHYAY: *An improved authentication and security scheme for LTE/LTE-A networks,* Journal of Ambient Intelligence and Humanized Computing, (2019), 1–23.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GURU JAMBHESHWAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
HISAR - 125001, HARYANA, INDIA
*E-mail address*: kkranga72@gmail.com

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GURU JAMBHESHWAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
HISAR - 125001, HARYANA, INDIA
*E-mail address*: yogeshchaba@yahoo.com