International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Enhanced Elliptic Curve Cryptography based Secure Transmission in LTE Network

Krishan Kumar, Yogesh Chaba

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

***Keywords*: EECC, OPSO, LTE, Communication, Security, Optimal key and eNodeB**

I. INTRODUCTION

Wireless network administrators today commit extensive manual exertion to arranging, designing, upgrading and keeping up their remote access systems. These endeavors have an incredible stake in their operational uses (OPEX). The institutionalization body third Generation Partnership Project (3GPP) has failed the principal arrivals of Evolved UTRAN, usually known as 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 [2]. Other than higher piece rate, lower inertness and numerous other administration contributions for LTE, user equipment (UE) control sparing is a significant issue [3].

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Krishan Kumar, Reseach Scholar, Department of computer Science & Engineering .Guru Jambheshwar University of Science & Technology, Hisar ,Haryana India

Dr. Yogesh Chaba, Professor in computer Science & Engg. Guru Jambheshwar University of Science & Technology, Hisar, Haryana India

LTE system is a low defer, all IP and high throughput organize. 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 [4]. LTE framework, called now and again super 3G, is required to offer a phantom proficiency between 2 to multiple times greater than 3GPP discharge six [5].

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 [6]. 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 [7]. 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 [9]. 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 [8]. Henceforth it additionally decreased the calculation power, memory and data transmission [10].

ECC is a lopsided encryption giving an equivalently high cryptographic quality in connection to the key sizes utilized [11]. There are numerous ECC systems are introduced in existing articles, for example, the ECC calculation, which makes the expense of computation, a little contrasted with different plans [12]. A protocol of key conveyance 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]. 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 [14].

In this paper, the procedure of encryption/decoding of an instant message in spatial area is outlined by upgrading security utilizing OPSO based ECC for better irregular number age.

Contributions of this work are described as follows:

- In this work, Enhanced Elliptic Curve Cryptography (EECC) is presented for securable transmission 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.
- In the platform of Network simulator (NS3), the presented EECC is implemented.
- The presented approach's performance based on energy efficiency, delay and delivery ratio is evaluated.

The remainder of the paper is made as looks for subsequent to: Following this presentation part, the related work in this space is reviewed and solidified into Section 2. Section 3 demonstrates the issues perceiving confirmation of existing strategies and fragment 4 contains review working model of proposed technique, ECC, OPSO calculation and stream graph. Fragment 5 presents result and talk part for instance coordinated assessments, obtained results and graphical depictions. Finally, the territory 6 wraps up the examination part of end.

II. LITERATURE REVIEW

Lately, Elliptic Curve Cryptography (ECC) has attained a lot of attention. Unlike RSA which requires a larger key size, which minimizes processing complexity, ECC provides the same protection to a smaller bit size. The ECC's encryption and encryption methods will work in the performance of the curve, but will not work in the messages. Based on the matrix approach for ECC, where high security is provided for encrypted messaging, **Balamurugan** *et al.* [15] have introduced a faster mapping system. At first, 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. Verilog code was utilized. The presented design is simulated and synthesized by FPGA.

To establish a secure connection and to encrypt the data, **Neha Tirtani** *et al.* [16] 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. Also the presence of sub exponential time complexity which makes cracking difficult adds more protection. So as to establish better connections, Diffie Hellman protocol has been utilized.

With the increasing growth in Device-to-Device (D2D) communication in 4G LTE-Advanced network, there occurs to critical issues such as availability and security. For achieving data security in D2D communications, a new secure data sharing protocol has been presented by **Zhang** *et al.* [17] 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. An important aspect of the proposed protocol is that by maintaining a record of the present status of the user's equipment (UE), a free-ride attack can be detected and not rejected by a key hint transmission between the UE and the developed NodeB, thereby enhancing availability of the system. Also, various delay models have been established in different application scenarios to search for optimal initial service providers to achieve the tradeoff between availability and cost. Detailed analysis and simulations show that the presented protocol was indeed an effective and practical solution of the secure data sharing mechanism for D2D communication.

For secure handover session key management through mobile relay on networks of LTE-A, **Qinglei Kong** *et al.* [18] presented a scheme. The proposed 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. Then, for minimizing the computational complexity and communication overhead, a novel proxy re-encryption approach was used, where the session keys were initially encrypted with the mobility management entity's (MME's) public key, re-encrypted by the mobile relay node (MRN), so that DeNBs can then decrypt session keys with their own keys without the direct involvement of the MME. On further Security Analysis, the proposed approach can successfully establish the session keys among on-board UEs and their associated DeNB, achieving forward and backward key separations, while resisting the collision among DeNB and MRN.

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. To alleviate these security weaknesses, Prabhat Kumar Panda and Sudipta Chattopadhyay [19] 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 employs 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.

III. PROBLEM DEFINITION

- A secure information sharing among gadgets without the association of GW and eNB, consequently totally offloading the phone system and participation is relied upon to be investigated in D2D correspondence. Progressively broad and entangled application situation in which the administration time isn't deterministic and abuses the impacts of versatility on security in D2D correspondence [17].
- 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 [19].

- During handover, a huge computational overhead and a long postponement may happen. Accordingly, the security research of gathering based correspondence in the span of handover will be an another test in LTE

All of these limitations influenced us to continue forward to the proposed system. The proposed procedure cleared out all the recently referenced issues.

IV. M ENHANCED ECC BASED SECURE TRANSMISSION IN LTE NETWORKS

A. *Overview*

In this work, User Equipment (UE) in the out of scope of eNB or base station speaks with the eNB. Thus, the source UE needs to transfer the information to eNB through the relay nodes in the LTE network. The source UE builds up data for transmission in LTE network. Long haul Evolution has a few disadvantages the extent that the security of this innovation is concerned. Especially, there are some security openings in validating clients for access in the space of Access Network. Secured data transmission in LTE is a big challenge, for that Enhanced Elliptic Curve Cryptography (EECC) is presented. The implementation of Elliptic Curve Cryptography by first transforming the message into an affine point on the Elliptic Curve, over the finite prime field. and 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. The whole working model of proposed method is demonstrated in fig.1.

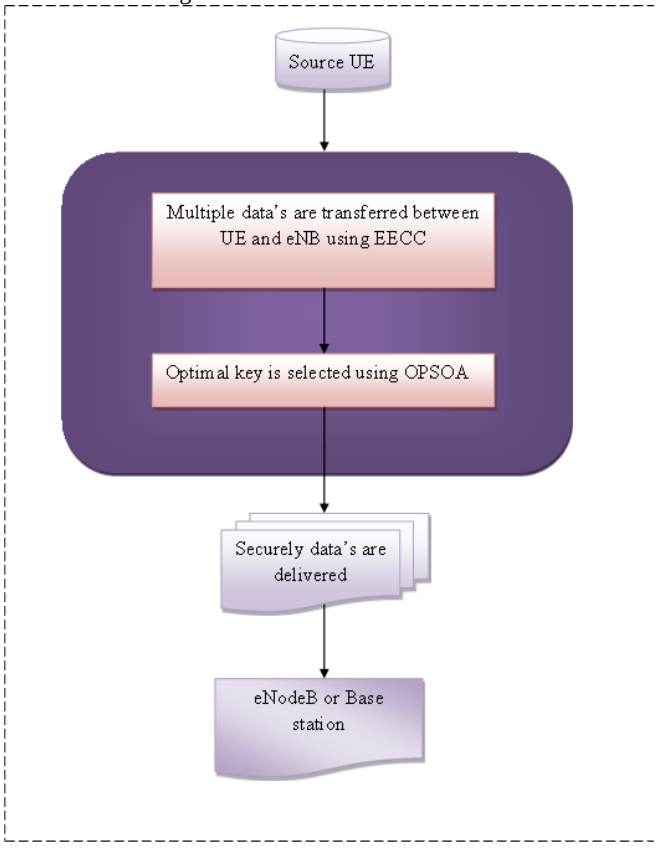
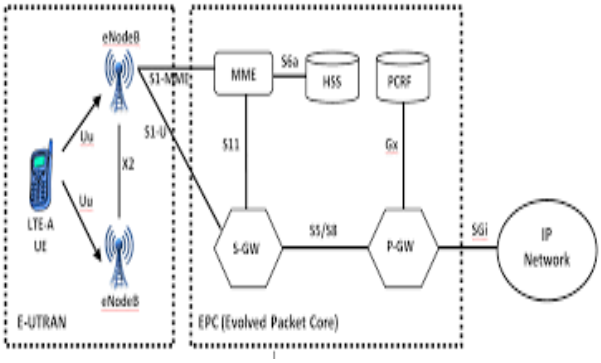


Fig.1 working model of proposed method

B. *LTE system model*

Fig. 2 demonstrates the system of the LTE network with the proposed methodology. All things considered, this design incorporates following parts: User Equipment (UE), advanced base stations or eNodeB (eNB), Home Subscriber Server (HSS), Packet data network Gateway or PDN Gateway (P-GW), Serving Gateway (S-GW) and Mobility Management Entity (MME). UE is a terminal which is utilized for communication. eNB which is utilized to control the cell phones in every cell. Interface between two eNB is meant as X2 which is utilized to advance the information during handover. Additionally, interface between the advanced packet centers is demonstrated as S1.HSS is a part goes about as a focal database to store the insights concerning endorsers in the network system. S-GW works as a switch, and transmits information between P-GW and eNB. P-GW interfaces with the outside condition i.e., it gives packet data to the UE. The interface between S-GW and P-GW is demonstrated as S5/S8 where S5 speaks to the interface between two gadgets in a similar system while S8 speaks to the interface between other two gadgets in various systems. As appeared on the fig.2, UEs those are in scope of eNB conveys legitimately to it. Generally the UEs forward the information demand by choosing the halfway relay nodes.



C. Transmission of data's between UE and eNB using EECC

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is an open key cryptography. An open key cryptography each source distributes the correspondence by and large have a couple of keys, specifically, open key and a private key. The public key will be generated utilizing this private key. Thus, to generate public key, Elliptic Curve Cryptography (ECC) is proposed. Nevertheless, by taking into account of key management, the ECC is enhanced by presenting Oppositional particle swarm optimization for choosing optimal private key.

Elliptic curve cryptography is a public key encryption process based on the hypothesis of elliptic curve, which is used to generate cryptographic keys that are more efficient, agile, and progressively smaller. Rather than the standard technique of generation resulting from the expansion of prime numbers, circular curve cryptography generates keys for the properties of the elliptic curve. 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 (fig.3) of ECC is given below,

$$P^2 = q^3 + \delta q + \Delta \quad (1)$$

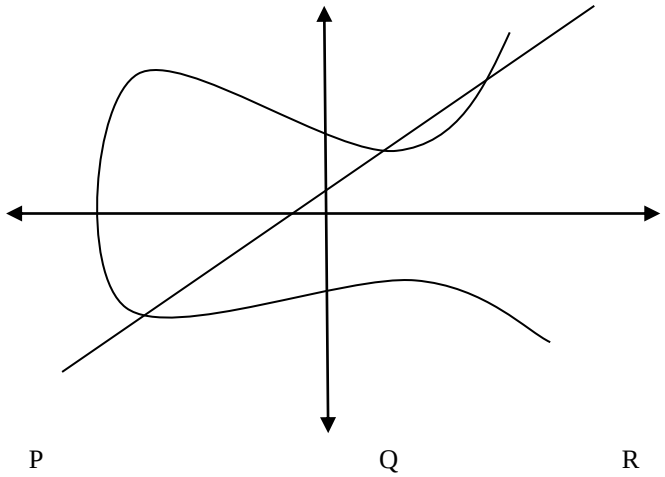


Fig.3 Elliptic curve cryptography

The key age procedure is utilized to produce the open key and private key. The ECC algorithm comprises of three stages as appeared in beneath;

(i) Key Generation

(ii) Encryption

(iii) Decryption

Key Generation:

The open key and private key generation is the significant procedures in key generation. Here, the sender encodes the data with the assistance of recipient's open key and collector unscrambles the data utilizing private key.

$$\Pr ivae\ key = R..V \times C.P \quad (2)$$

Where, R.V denoted as Random Values and C.P is represented as Curve Point.

Encryption

Encryption procedure is utilized to change over the first data into various structures which is utilized to build the security. For encryption, the info data is given to Elliptic Curve Cryptography algorithm which changes over the data and given the encoded data e.i. In this Elliptic Curve Cryptography (ECC), the yield is part into two cipher texts as Ct1 and Ct2.

$$C_{t1} = \eta \times f \quad (3)$$

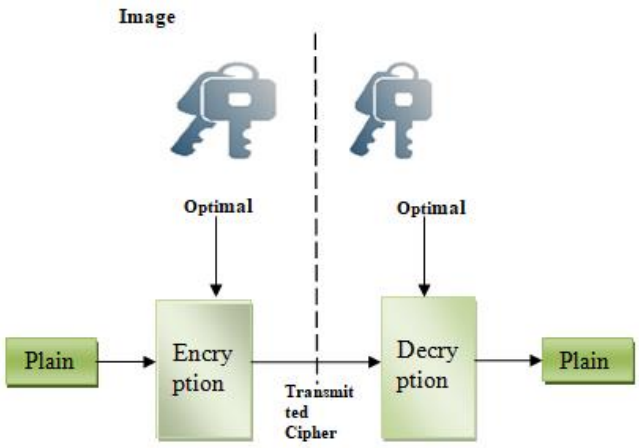
$$C_{t2} = e.i + \eta \times f \quad (4)$$

Where, C_{t1}- ciphers text 1, C_{t2}-cipher text 2, η- key value and e.i-encryption information.

Decryption

After the encryption procedure, the scrambled data Ct1 and Ct2 is sent to the beneficiary. At that point, in beneficiary side, the scrambled data is unscrambled utilizing condition (5). The process of ECC is described in fig.3,

$$O = C.P_2 - x \times C.P_1 \quad (5)$$



D. Optimal Key Selection using OPSOA

In this area, the idea of opposition based optimization is implanted in the PSO. In this work, ECC algorithm is improved or optimized by utilizing Oppositional Particle Swarm Optimization (OPSO) algorithm. This algorithm is utilized to create the optimal key qualities. As the quantity of transmissions is happened through the various ways, information rate of the system's rate of information is enhanced. In any case, a couple routing paths may lose its security and furthermore they are exposed to obstruction of between ways. Thus, to defeat these issues, an optimal key to be chosen from the quantity of keys. For ideal key choice, OPSO is presented. This algorithm's steps are depicted as pursues:

Initialization

The proposed way to deal with initialization of population utilized the resistance based strategy in which the inputs are population and its opposite population. The candidate solution of this method is optimal key between source UE and eNB. Initialization of the solutions can be indicated as,

$$p_{Nn} = p_{N1}, p_{N2}, \ldots\ldots\ldots\ldots\ldots p_{Ni} \quad (6)$$

Here, p_{Nn} represents the prime numbers of n^{th} population. d- Denoted as number of dimensions

Where, i=1, 2, 3……..d,

Fitness calculation

After the swarms or optimal key's initialization, the particle swarm's fitness is evaluated. It is defined as the function that measures a solution's optimality and generally it is the objective function. The fitness capacity is characterized dependent on the throughput of the solution in this methodology for optimal key or private key choice. The proportion between the size of the plaintext and the encryption times is characterized as the throughput of the arrangement. It is determined by utilizing the accompanying condition.

$$Thr_n = \frac{Size\ of\ \ plain\ text}{Encryption\ time} \quad (7)$$

Throughput of 09f nth solution is represented as Thr_n. Fitness function of solution is calculated as

$$Fitness = Max\{thr_n\} \quad (8)$$

Every particle in the swarm handles d-dimensions' three attributes such as,

Local best (l-best):

It is the best position in which a particle has visited yielding the highest value of fitness for that particle. For a minimization task, this worth can be smallest.

Global best (g-best):

It is where the best wellness is accomplished by any molecule of the swarm developed up until this point.

Updation function

After calculating the fitness to the position of the swarm, it will be updated to the next position. Depend on the modified performances such as global best and local best, the particle swarm is updated to next position. These performances are described as follows:

Velocity Update:

Velocity is a d-dimensional vector that decides the development speed and heading of the particle. The velocity is updated by the accompanying condition given below,

$$V_{i+1} = wV_i + C_1 rand(0,1)K_{lbest} - K_i + C_2 rand(0,1)K_i \quad (9)$$

Where w is the inertia weight, C1 and C2 are the constant coefficients; Klbest and Kgbest are the local and global bests of the keys.

Position Update:

Every particle refreshes its position to move in the solution hyperspace looking for optimal solution. Every one of the particles in a swarm moves stochastically for optimal positions and update their positions utilizing the accompanying condition,

$$K_{i+1} = k_1 + V_i \quad (10)$$

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.

Algorithm: Opposition Particle Swarm Optimization

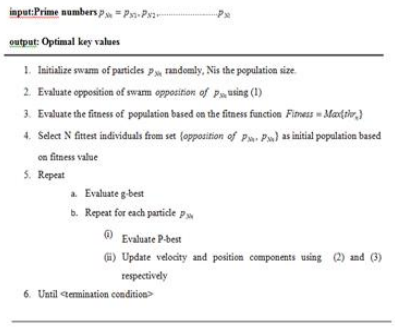


Table_1 of Algorithm

Parameters	Values
eNB coverage area	Circular with radius=375m with one cell
System Bandwidth	10MHz
Transmit Power	43dBm
Receiver Sensitivity	-110 dBm
Number of UEs	30
Area	1000×1000m
eNBs Distance	400m
Routing protocol	AOMDV
Simulation time	100s

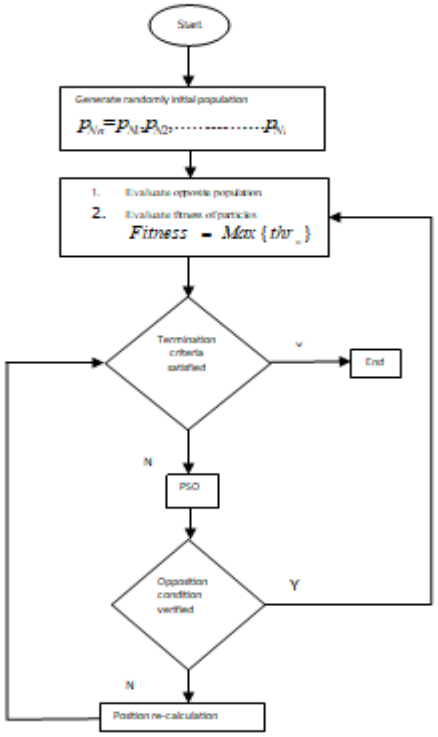


Fig 4.Flow Chart of OPSO for Optimization

E. Result and Discussion

This proposed OPSO based ECC is executed in the Network Simulator-3 (NS3). In this recreation, 30 UEs are exhibited and are moving in 1000×1000m reproduction region. Two eNBs are performing with the inclusion of 375m. These two eNBs keep separation with 400m. Transmit intensity of every terminal in the system is 43dBm. For bundle steering, AOMDV directing convention is introduced. With these parameters, the proposed methodology is reenacted inside 100 seconds. Table 1 demonstrates the reenactment parameters and its qualities.

F. Evaluation metrics

The process of the proposed approach is evaluated by using the following metrics. The Performance metrics of our proposed approach OPSO based ECC is compared with that of existing method ECC.

End to End delay

The delay of system portrays to what extent the system takes to transmit a bit to the destination. The Unit of this parameter is estimated in milliseconds (ms).

Delivery ratio

It is the proportion of the quantity of packets got effectively and the aggregate sum of packets transmitted. Unit of this parameter is estimated in packets/s.

$$D.r = \frac{No.of\ \ packets\ rxd}{Amount of\ \ packets\ txd}$$

G. Execution dependent on number of clients

Execution measurements of the proposed methodology OPSO-ECC are assessed for various numbers of users such as 10, 15, 20, 25 and 30. Figures 5 and 6 demonstrate the examination of the presentation measurements of OPSO-ECC with the past work ECC. Figure 5 demonstrates the comparison of delivery ratio of OPSO-ECC with the current procedures, for example, ECC for various numbers of users. Contrasted with ECC, conveyance proportion of the proposed OPSO-ECC is expanded from 70%. Most extreme conveyance proportion of our proposed technique is 97%. Be that as it may, existing strategy reach as limit of ECC 60%. Examination of deferral of the proposed methodology with ECC is appeared in figure 6. Delay of the proposed OPSO-ECC is diminished up to 200ms yet existing techniques min postponement is 400ms. From the diagrams we have obviously realized that our proposed strategy got min delay and great delivery ratio.

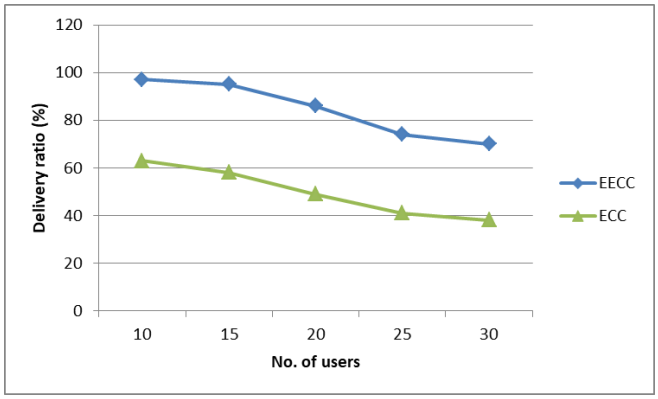


Fig.5 demonstrates delivery ratio Vs No. of users

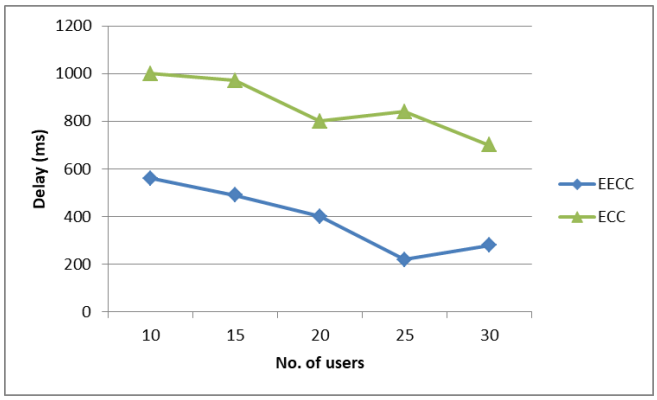


Fig.6 demonstrates No. of users Vs delay

Performance metrics of the proposed approach OPSO-ECC are evaluated for varying simulation time 20-100 seconds. Figures 7 and 8 show the comparison of the performance metrics of OPSO-ECC with the previous work ECC. Figure 7 shows the comparison of delivery ratio of OPSO-ECC with the existing methods such as ECC for varying simulation time. Compared to ECC, the maximum delivery ratio of proposed OPSO-ECC is 98%. Comparison of delay between proposed approaches with existing ECC is shown in figure 8. Delay of the proposed OPSO-ECC is decreased to 15% than that of OFF method ECC.

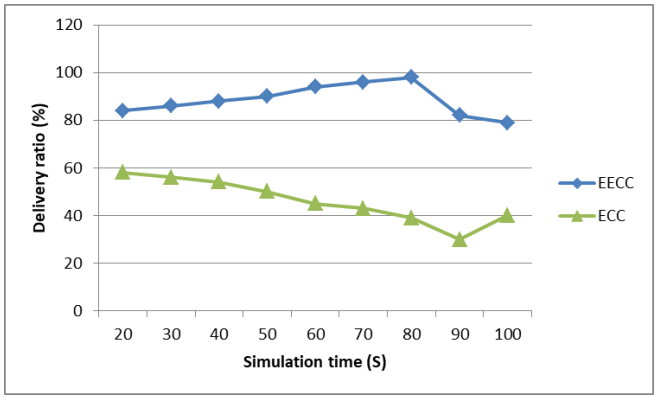


Fig.7 demonstrates delivery ratio Vs simulation time

V. 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. If the customer is in out of range from the base station needs to speak with the base station. Nevertheless, the correspondence must be verified. Along these lines, EECC is introduced in this work. It is prominent that elliptic twist cryptosystem (ECC) based calculation would be best choice as a result of their little key sizes and capable figurings. The ECC calculation is overhauled or upgrades by using Oppositional Particle Swarm Optimization (OPSO) calculation and moreover the OPSO is used to deliver the perfect key characteristics. The proposed EECC is completed in the phase of Network test framework (NS3).

Itemized assessments of execution represent that the proposed strategy accomplishes better execution as far as vitality productivity, conveyance proportion and postponement contrasted and existing strategies. From the diagrams, we have obviously realized that the proposed EECC is outperformed.

REFERENCES

1. Schmelz, Lars Christoph, Mehdi Amirijoo, Andreas Eisenblaetter, Remco Litjens, Michaela Neuland, and John Turk, "A coordination framework for self-organisation in LTE networks," In 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops, pp. 193-200, 2011.
2. Piro, Giuseppe, Luigi Alfredo Grieco, Gennaro Boggia, Rossella Fortuna, and Pietro Camarda, "Two-level downlink scheduling for real-time multimedia services in LTE networks," IEEE Transactions on Multimedia, Vol. 13, No. 5, pp. 1052-1065, 2011.
3. Capozzi, Francesco, Giuseppe Piro, Luigi Alfredo Grieco, Gennaro Boggia, and Pietro Camarda, "Downlink packet scheduling in LTE cellular networks: Key design issues and a survey, " IEEE Communications Surveys & Tutorials, Vol. 15, No. 2, pp. 678-700, 2012.
4. Sevindik, Volkan, Jiao Wang, Oguz Bayat, and Jay Weitzen, "Performance evaluation of a real long term evolution (LTE) network," In 37th Annual IEEE Conference on Local Computer Networks-Workshops, pp. 679-685, 2012.
5. Nasri, Ridha, and Zwi Altman, "Handover adaptation for dynamic load balancing in 3GPP long term evolution systems," arXiv preprint arXiv:1307-1212, 2013.
6. Gampala, Veerraju, Srilakshmi Inuganti, and Satish Muppidi, "Data security in cloud computing with elliptic curve cryptography," International Journal of Soft Computing and Engineering (IJSCE), Vol. 2, No. 3, pp. 138-141, 2012.
7. Vigila, S. Maria Celestin, and K. Muneeswaran, "Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications," IJ Network Security, Vol. 14, No. 4, pp. 236-242, 2012.
8. Yoon, Eun-Jun, and Kee-Young Yoo, "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem," The Journal of supercomputing, Vol. 63, No. 1, pp. 235-255, 2013.
9. Amounas, F., and E. H. El Kinani, "An efficient elliptic curve cryptography protocol based on matrices," International Journal of Engineering Inventions, Vol. 1, No. 9, pp. 49-54, 2012.
10. Shen, Jian, Haowen Tan, Sangman Moh, Ilyong Chung, Qi Liu, and Xingming Sun, "Enhanced secure sensor association and key management in wireless body area networks," Journal of Communications and Networks, Vol. 17, No. 5, pp. 453-462, 2015.
11. Höller, Andrea, Norbert Druml, Christian Kreiner, Christian Steger, and Tomaz Felicijan. "Hardware/software co-design of elliptic-curve cryptography for resource-constrained applications." In 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1-6. IEEE, 2014.
12. Qiu, Yue, Maode Ma, and Xilei Wang, "A proxy signature-based handover authentication scheme for LTE wireless networks," Journal of Network and Computer Applications, Vol. 83, pp. 63-71, 2017.
13. Louw, J., G. Niezen, T. D. Ramotsoela, and Adnan M. Abu-Mahfouz, "A key distribution scheme using elliptic curve cryptography in wireless sensor networks," In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN), pp. 1166-1170, 2016.
14. Lai, Chengzhe, Hui Li, Rongxing Lu, and Xuemin Sherman Shen, "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks," Computer Networks, Vol. 57, No. 17, pp. 3492-3510, 2013.
15. Balamurugan, R., V. Kamalakannan, Ganth D. Rahul, and S. Tamilselvan, "Enhancing security in text messages using matrix based mapping and ElGamal method in elliptic curve cryptography," In 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 103-106, 2014.
16. Tirthani, Neha, and R. Ganesan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," IACR Cryptology ePrint Archive, Vol. 49, 2014.
17. Zhang, Aiqing, Jianxin Chen, Rose Qingyang Hu, and Yi Qian, "SeDS: Secure data sharing strategy for D2D communication in LTE-Advanced networks," IEEE Transactions on Vehicular Technology, Vol. 65, No. 4, pp. 2659-2672, 2015.
18. Kong, Qinglei, Rongxing Lu, Shuo Chen, and Hui Zhu, "Achieve secure handover session key management via mobile relay in LTE-advanced networks," IEEE Internet of Things Journal, Vol. 4, No. 1, pp. 29-39, 2016.
19. Panda, Prabhat Kumar, and Sudipta Chattopadhyay, "An improved authentication and security scheme for LTE/LTE-A networks," Journal of Ambient Intelligence and Humanized Computing, pp. 1-23, 2019.

AUTHORS PROFILE

Krishan Kumar, Reseach Scholar in Department of computer Science & Engineering .Guru Jambheshwar University of Science & Technology, Hisar ,Haryana (India) in Mobile Communication area.
E-mail:- kkranga72@gmail.com

Dr. Yogesh Chaba, Professor in computer Science & Engg. Guru Jambheshwar University of Science & Technology, Hisar, Haryana (India),in Mobile Communication area and Computer Networking ,Wireless sensor network. More than 400 research papers International / National levels.
E-Mail:- yogeshchaba@yahoo.com