**AN OPTIMIZED SECURITY PROTOCOL FOR D2D COMMUNICATION IN LTE-A NETWORK**

**A PROJECT REPORT**

*Submitted in partial fulfillment of the*

*Requirement for the award of the*

*Degree of*

**BACHELOR OF TECHNOLOGY**

**IN**

**ELECTRONICS AND COMMUNICATION ENGINEERING**

*by*

SUMANTH A - 17BEC1190

AYAN NATH - 17BEC1051

PRAVEEN G - 17BEC1105

*Under the Guidance of*

**Dr. Vijayakumar P**

****

SCHOOL OF ELECTRONICS ENGINEERING

VELLORE INSTITUTE OF TECHNOLOGY

CHENNAI - 600127

**June 2020**

***CERTIFICATE***

This is to certify that the Project work titled “***An Optimized Security Protocol For D2D Communication In LTE A - Network*** ” that is being submitted by ***Sumanth A (17BEC1190)***, ***Ayan Nath(17BEC1051) and Praveen G(17BEC1105)*** is in partial fulfillment of the requirements for the award of **Bachelor of Technology in Electronics and Communication Engineering**, is a record of bonafide work done under my guidance. The contents of this Project work, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

**Dr. VIJAYAKUMAR P**

**Guide**

**The thesis is satisfactory / unsatisfactory**

**Internal Examiner External Examiner**

Approved by Approved by

**PROGRAM CHAIR** **DEAN**

B. Tech. Electronics and Communication School of Electronics & Engineering Engineering

**ACKNOWLEDGEMENTS**

I sincerely thank my Dean, Dr. Siva Subramanian, Program Chair for their support and providing us with the required facilities to complete this project.

## This acknowledgement of gratitude gives us an opportunity to thank all those who have lent us a helping hand. This project has been a product of motivation and encouragement from various sources. We would like to place on record my deep gratitude towards Dr.Vijayakumar P who gave us the opportunity to work under him.

Sumanth A Ayan Nath Praveen G

17BEC1190 17BEC1051 17BEC1105

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **S. No.** | **SUB- HEADING** | **NAME** | **PAGE NO.** |
|  |  | ACKNOWLEDGEMENT | 3 |
|  |  | ABSTRACT | 5 |
| 1 | 1.1  1.2  1.3  1.4  1.5 | INTRODUCTION  LTE Advanced  D2D Communication  D2D Applications  Optimized Security Protocol for D2D Communication in LTE Advanced  Contribution of the authors | 6  6  7  8  8  9 |
| 2 | 2.1 | LITERATURE SURVEY  Literature review | 10  10 |
| 3 | 3.1  3.2  3.3  3.4  3.5 | CONVENTIONAL SECURE DATA SHARING PROTOCOL LTE-A NETWORKS  Background  Network Architecture and Threats for Conventional Protocol System  Initialization of SeDS Protocol System  Sharing of Data using SeDS Protocol System  Discussion of randomness of the generated key | 11  12  13  14  15  15 |
| 4 | 4.1  4.2  4.3  4.4  4.5 | SIMULATION RESULTS AND IT’S DISSCUSSION  Overview  Algorithm  Flowchart  Overall Code  Results with Description about figures | 16  17  18,19  20  21-23  23-26 |
| 5 |  | CONCLUSION AND FUTURE WORKS  References | 27  28 |

**ABSTRACT**

Third Generation Partnership Projects (3GPP) introduced fourth generation of wireless communication entitled Long Term Evolution- Advanced (LTE-A). Security always plays a vital role in Communication. Device to device (D2D) Communication in LTE-A in between user equipment can be carried out using Secure Data Sharing Strategy (SeDS) via evolved Node B (eNB) and Gateway (GW). But, Communication between eNB and GW is not secure. And if this part of system will not be secure, further communication may get hampered. In this paper, implementation of optimized protocol has been shown. Due to this protocol, security in between communication of eNB and GW will be enhanced.

Keywords— Long Term Evolution Advanced (LTE-A) network, Security, Device to Device (D2D), Secure Data Sharing Strategy (SeDS).

**Keywords: 433 MHz Transceiver, PICamera, Raspberry Pi, Internet of Things**

**CHAPTER I**

**INTRODUCTION**

**1.1 LTE Advanced**

**LTE Advanced** is a mobile communication standard and a major enhancement of the Long-Term Evolution (LTE) standard. It was formally submitted as a candidate 4G to ITU-T in late 2009 as meeting the requirements of the IMT-Advanced standard, and was standardized by the 3rd Generation Partnership Project (3GPP) in March 2011 as 3GPP Release 10.[[1]](https://en.wikipedia.org/wiki/LTE_Advanced#cite_note-1)

The LTE format was first proposed by NTT DoCoMo of Japan and has been adopted as the international standard. LTE standardization has matured to a state where changes in the specification are limited to corrections and bug fixes. The first commercial services were launched in Sweden and Norway in December 2009 followed by the United States and Japan in 2010. More LTE networks were deployed globally during 2010 as a natural evolution of several 2G and 3G systems, including Global system for mobile communications (GSM) and Universal Mobile Telecommunications System (UMTS) in the 3GPP family as well as CDMA2000 in the 3GPP2 family.

The work by 3GPP to define a 4G candidate radio interface technology started in Release 9 with the study phase for LTE-Advanced. Being described as a 3.9G (beyond 3G but pre-4G), the first release of LTE did not meet the requirements for 4G (also called IMT Advanced as defined by the International Telecommunication Union) such as peak data rates up to 1 Gb/s. The ITU has invited the submission of candidate Radio Interface Technologies (RITs) following their requirements in a circular letter, 3GPP Technical Report (TR) 36.913, "Requirements for Further Advancements for E-UTRA (LTE-Advanced)." These are based on ITU's requirements for 4G and on operators’ own requirements for advanced LTE. Major technical considerations include the following:

* Continual improvement to the LTE radio technology and architecture
* Scenarios and performance requirements for working with legacy radio technologies
* Backward compatibility of LTE-Advanced with LTE. An LTE terminal should be able to work in an LTE-Advanced network and vice versa. Any exceptions will be considered by 3GPP.
* Consideration of recent World Radiocommunication Conference (WRC-07) decisions regarding frequency bands to ensure that LTE-Advanced accommodates the geographically available spectrum for channels above 20 MHz. Also, specifications must recognize those parts of the world in which wideband channels are not available.

Likewise, 'WiMAX 2', 802.16m, has been approved by ITU as the IMT Advanced family. WiMAX 2 is designed to be backward compatible with WiMAX 1 devices. Most vendors now support conversion of 'pre-4G', pre-advanced versions and some support software upgrades of base station equipment from 3G.

The mobile communication industry and standards organizations have therefore started work on 4G access technologies, such as LTE Advanced. At a workshop in April 2008 in China, 3GPP agreed the plans for work on Long Term Evolution (LTE).[[5]](https://en.wikipedia.org/wiki/LTE_Advanced#cite_note-5) A first set of specifications were approved in June 2008.[[6]](https://en.wikipedia.org/wiki/LTE_Advanced#cite_note-6) Besides the peak data rate 1 Gb/s as defined by the ITU-R, it also targets faster switching between power states and improved performance at the cell edge. Detailed proposals are being studied within the working groups.

Three technologies from the LTE-Advanced tool-kit – carrier aggregation, 4x4 MIMO and 256QAM modulation in the downlink – if used together and with sufficient aggregated bandwidth, can deliver maximum peak downlink speeds approaching, or even exceeding, 1 Gbit/s. Such networks are often described as ‘Gigabit LTE networks’ mirroring a term that is also used in the fixed broadband industry.

**1.2 D2D Communication**

Device-to-Device (D2D) communication in cellular networks is defined as direct communication between two mobile users without traversing the Base Station (BS) or core network. D2D communication is generally non-transparent to the cellular network and it can occur on the cellular frequencies (i.e., inband) or unlicensed spectrum (i.e., outband).

In a traditional cellular network, all communications must go through the BS even if communicating parties are in range for proximity-based D2D communication. Communication through BS suits conventional low data rate mobile services such as voice call and text messaging in which users are seldom close enough for direct communication. However, mobile users in today's cellular networks use high data rate services (e.g., video sharing, gaming, proximity-aware social networking) in which they could potentially be in range for direct communications (i.e., D2D). Hence, D2D communications in such scenarios can greatly increase the spectral efficiency of the network. The advantages of D2D communications go beyond spectral efficiency; they can potentially improve throughput, energy efficiency, delay, and fairness.

**1.3 D2D Applications**

D2D Communications is used for

1. **Local Services:** In local service, user data is directly transmitted between the terminals and doesn't involves network side, e.g. social media apps, which are based on proximity service.
2. **Emergency communications:** In case of natural disasters like hurricanes, earthquakes etc., the traditional communication network may not work due to the damage caused. Ad-hoc network can be established via D2D which could be used for such communication in such situations.
3. **IoT Enhancement:** By combining D2D with Internet of things (IoT), a truly interconnected wireless network will be created. Example of D2D-based IoT enhancement is vehicle-to-vehicle (V2V) communication in the Internet of Vehicles (IoV). When running at high speeds, a vehicle can warn nearby vehicles in D2D mode before it changes lanes or slows down.

**1.4 Optimized Security Protocol for D2D Communication in LTE Advanced**

Huge demand of broadband wireless communication data and various multimedia applications obligate to carry out fast improvement in the sector of wireless network. Enormous users want to access the network from any place and at any time via their devices. LTE-A has been developed to fulfil the demand of wireless communication network and its user’s. But, with the establishment of communication using LTE-A network, security and confidentiality are the key factors which should get focussed. In the year of 2014, a group-based security protocol was proposed for LTE-A but it was for machine type communication (MTC). The protocol was implemented in concern with security and performance for MTC. Device to device (D2D) communication in cellular network enables to establish direct communication between two mobile users or nearby mobiles without extending across the Base station (BS) or core network. Hence, D2D communication is considered as one of the best ways out for data offloading. Furthermore, it also delivers some unique features such as making use of information between critical public safety networks and appearing commercial networks based on LTE. Ultimately, it helps to achieve significant performance and efficiency benefits in LTE network. As LTE-A network operates on a licensed band; it delivers a systematic and planned deployment which results in a better user satisfaction and quality of service. Hence, it is keenly required to develop an optimized protocol for the combination of LTE-A network with D2D communication to provide better security.

**1.5 Contribution of the authors**

Each of the three authors have contributed equally in the project. It starts from software coding to execution. The work has been equally shared by each of the authors.

**CHAPTER II**

**LITERATURE SURVEY**

**2.1 Literature review**

Detailed study on integration of D2D communication in LTE-A network has been done. It has been found out that, most of them have researched on service quality, network congestion, pricing scheme, seamless offloading, mobility of relay and joint neighbor parameters. A very few researchers have considered security for research. One associated paper for security in D2D communication with LTA network has revealed that how secure communication can be established in between two user equipments via eNB and GW. But some loopholes are present in the proposed system which results into lack of confidentiality during the communication. The most similar kind of study of this paper has been done in various wireless networks such as in wireless body area networks (WBANs) and vehicle ad hoc networks (VANETs). To achieve security in terms of access controls in WBANs, symmetric cryptography is implemented. On the other hand, public key infrastructure (PKI) is responsible to establish security requirements in VANETs. Using combination of both symmetric cryptography and PKI, one protocol is designed to achieve security in D2D communication between two user equipments in LTE-A networks. By jointly considering all the points, we attempt to design one protocol where integration of symmetric cryptography, PKI and elliptic cryptography curve. Analysis of previous papers where D2D communication is implemented in LTE network can be summarized through table no. 1.

Table 1. Previous Research Review of D2D Communication with LTE-A network

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr.No.** | **Title of Paper** | **Advantages** | **Disadvantages** |
| 1 | When D2D communication improves group oriented services in beyond 4G networks (2015) [3] | Improving service quality in terms of delay and energy consumption | Security. |
| 2 | Secure and Smart Media Sharing Based on a Novel Mobile Device-to-Device Communication Framework with Security and Procedures (2015) [4] | Reduced Network Congestion and Better Pricing Scheme | Security and Reliability. |
| 3 | Secure data sharing strategy for D2D communication LTE-Advanced networks (2015) [5] | Secure data and Sharing mechanism. | Communication between eNB and GW is not secured. |
| 4 | Efficient Load Balancing using D2D Comm. and Biasing in LTE-Advance Het-Nets (2015) [6] | Seamless offloading and mobility of the relay. | Implemented for one macro base station only. |
| 5 | Enabling D2D Communications Through Neighbour Discovery in LTE Cellular Networks (2015) [7] | Neighbour Discovery and Joint neighbour detection. | orthogonality of Ψ cannot be preserved |

**CHAPTER III**

**CONVENTIONAL SECURE DATA SHARING PROTOCOL LTE-A NETWORKS**

**3.1 Background**

Secure Data Sharing Strategy (SeDS) protocol was implemented to provide the D2D communication in LTE-A networks. This system combines the advantages of public key cryptography and symmetric encryption. The proposed protocol helps to achieve security and availability parameter in D2D communication. Detail analyses on D2D communication in comparison with WBAN’s and VANET’s have also been done. For this investigation, two parameters have been focussed entitled as Public Key Infrastructure (PKI) and Symmetric Encryption. The conclusion of the analysis is yet in D2D, PKI and symmetric encryption is not implemented. But this is not the case in regards with WBAN’s and VANET’s. Implementation of PKI and symmetric encryption is available in both the cases.

**3.2 Network Architecture and Threats for Conventional Protocol System**

Network architecture for SeDS protocol system includes four important parts, gateway (GW), evolved node B (eNB), User Equipments (UE’s) and Service Providers (SP’s). Out of which, eNB and GW are assumed to be trustworthy which will not get affected by attacker. D2D communication usually gets attacked by free riding attack, which ultimately reduces the system availability and privacy preservation in terms of security. The proposed SeDS protocol is based on two preliminaries known as Bilinear Pairing and Diffie-Hellman Key Exchange (DHKE).

**3.3 Initialization of SeDS Protocol System**

System initialization of SeDS protocol is done through four steps such as system parameter generation, SP registration, UE registration and system setup. System parameter generation step is used for generation of tuple (q, g, g1, G, GT, ế) by using function Gen (K). Also, selection of secure symmetric encryption algorithm Encs () and two hash function H0 and H1 is done by eNB in this step only. In second step that is in SP registration, registration of real identity (RID0) is done so that it will be able to provide original data in the system. Then, calculation of PID0 is done using PID0 = H0 (RID0). PID0 is known as pseudo identity for SP. Finally calculation of Private and Public key will be done (X0, x0) and it will be sent to SP by eNB through secure channel. To minimise overhead of communication, SP and UE both calculate their pseudo identity by their own. SP registration will be done exactly similar to UE registration. Moving towards the last step which is System setup, it plays a very important role in system initialisation. In this step, eNB is used to keep a record of various parameters such as RID, PID, Public Key, Portion Index (Pi), Share Frequency and Malicious behaviour amount. Also, to check original data, combined record of Pi and Payload (M) is stored by eNB. Furthermore, for the sake of data authority and integrity, computation of signature σ1 is done by SP and will be attached with Pi and M. The whole process is completed online so that data sharing latency will be minimised.

**3.4 Sharing of Data using SeDS Protocol System**

Once the initialisation of the system is finished, one needs to focus on how data sharing is carried out using the SeDS protocol system. To understand data sharing we need to consider two user equipments known as UEi and UEj, one eNB and one GW. The whole process is divided into 8 steps.

* The 1st step is known as “Service Request”. In this step, UEi(who wants to have ith  frame of data), chooses c (where, c ϵ to Zq\*) and calculates key hint z (where z = gc) so that communication key Kc will be generated. Also, this step calculates HMAC (Internet Standard RFC 2104) of message M using hash function of parallel combination of K+ ⊕ opad, H(K+ ⊕ ipad) and m. Where

K+ is the key padded out to size

opad = 0011 0110, 0011 0110 and so on

ipad = 0101 1100, 0101 1100 and so on

Finally, service request message will be sent to eNB, which includes whole HMAC message with its PIDi, z and the expected Pi.

* The second step is entitled as “Authentication”, after receiving request message authenticity will be checked by eNB by calculating hash value of message. If it is found to be authenticated, it will be checked that whether it is available in record table or not. If it is available it will be ignored and if not the message will be dent to GW with its RIDi followed by that the third step will be performed which is called as “Candidate Detection”. In this step, detection of valid D2D pair is done for requesting UE by Proximity Service Control Function (PSCF) and finally gateway sends to eNB with its RIDj.
* The next step is known as “Pair Selection”. This step as its name suggests, performs the proper selection of the candidate with which Pi will match. Sending of request message to selected entity and acknowledgement of it will also be done in this step only. The real data transmission process starts with next step called as “Data Transmission”. Once request message is received encryption of message will be done to recover original message and it will be sent with signature σ2. The whole message is obtained in the format of PIDi, PIDj, Pi, Enc (M) (M’), Time Stamp (Ts), Signature (σ1) and Signature (σ2). Finally this message will be sent from transmitter to eNB so that its shared frequency record will be updated.
* The further step is called as “Entity Verification”. In this step, after receiving packet extraction of PIDj will be done by UEi from message. Followed by that, comparison of PIDj and pseudo identity will be done. IF match is obtained, packed will be dropped. If not, checking will be done by verifying the balance of the following equation. If encryption of Xj and hash function of parallel combination of PIDj, Pi, M’, Ts and σ1 isequal to encryption of σ2, g then it confirms that the data is send by entity with pseudo identity PIDj. In this step, for the sake of timestamp Ts, eNB verifies that the message is sent within the allowable time window or not. If it is so, decryption of message will be carried out and feedback will be recorded.
* The seventh step is known as “Data Verification”. To check data authority, encryption of X0 and hash function of parallel combination of Pi and M is calculated. Also, encryption of σ1 and g is calculated. If both the values are found to be equal, then the data will be considered to be authorised. And if not then it is considered as impersonation attack.
* The last step is “Record Refresh”, here eNB verifies the validity of σ1 and if it is found to the valid PIDi column in record table will get refreshed by inserting Pi and also shared frequency of PIDj will be incremented by 1 and if σ1 is not found to be valid the malicious behaviour amount record will be updated. In this way, whole SeDS protocol system is implemented to achieve security.

While dealing with such scenario, the most crucial part is to select proper device to which we want to send information. We have seen the device detection is done by GW and the RID of selected device is sent to eNB. But here the drawback of the system is that the communication between eNB and GW is not secure. It can be shown through figure 1. If this part of the system is not secure the further communication will be no more authentic. Hence, to achieve security between eNB and GW a new idea has been proposed. It is explained in the next section.

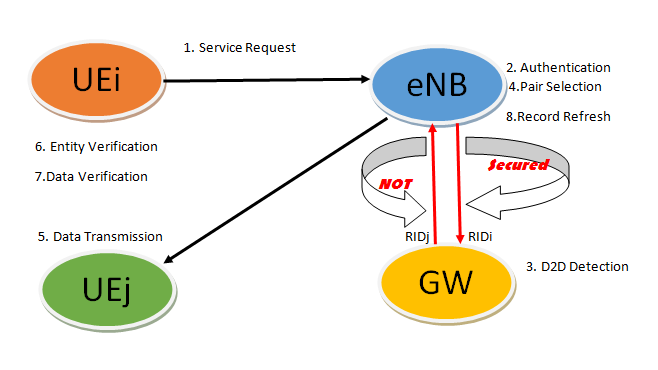


Fig.1. Conventional SeDS Protocol System for D2D Communication in LTE-A Network

**3.5 DISCUSSION ON RANDOMNESS OF THE GENERATED KEY**

* When ECC is implemented in between eNB and GW to achieve security, its intensity depends on the generated random key. Hence, it is necessary to check proportion of randomness of key. For the randomness properties of produced key, it needs to get accurate statistical results. If 100 binary sequences were tested, 96 binary sequences had P-values which will be less than or equal to 0.1. Hence, the proportion obtained will be 96/100=0.96. NIST, a statistical test is used to analyze the randomness of the key. Following figure 3 indicates how many samples have passed the given tests. The following simulation results have shown that the generated random key sequences pass all the tests and ultimately maintained its randomness and uniformity.

**CHAPTER IV**

**SIMULATION RESULTS AND IT’S DISSCUSSION**

**4.1 Overview**

Elliptic Curve Cryptography has been a recent research area in the field of Cryptography. It provides higher level of security with lesser key size compared to other Cryptographic techniques. A new technique has been proposed in this paper where the classic technique of mapping the characters to affine points in the elliptic curve has been removed. The corresponding ASCII values of the plain text are paired up. The paired values serve as input for the Elliptic curve cryptography. This new technique avoids the costly operation of mapping and the need to share the common lookup table between the sender and the receiver. The algorithm is designed in such a way that it can be used to encrypt or decrypt any type of script with defined ASCII values.

Cryptography is transformation of plain message to make them secure and immune from intruders. Elliptic Curve Cryptography (ECC) is a public key cryptography developed independently by Victor Miller and Neal Koblitz in the year 1985. In Elliptic Curve Cryptography we will be using the curve equation of the form

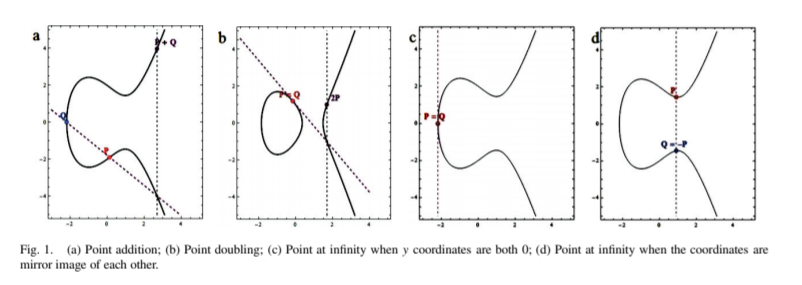
**y2 = x 3 + ax + b**

which is known as Weierstrass equation, where a and b are the constant with

**4a3 + 27b2 = 0**

Cryptographic operation on elliptic curve over finite field are done using the coordinate points of the elliptic curve. Elliptic curve over finite field equation is given by:

**y2 = {x 3 + ax + b} mod {p}**



The two point P(x1, y1) and Q(x2, y2) are distinct. P + Q = R(x3, y3) is given by the following calculation. Figure 1(a) shows graphical representation of Point Addition operation.

**x3 = {λ2 − x1 − x2} mod p**

**y3 = {λ(x1 − x3) − y1} mod p**

where

**λ = y2 − y1 x2 − x1 mod p**

The two point P(x1, y1) and Q(x1, y1) overlap. P + Q = R(x3, y3) is given by the following calculation. Figure 1(b) shows graphical representation of Point Doubling operation.

**x3 = {λ2 − 2x1} mod p**

**y3 = {λ(x1 − x3) − y1} mod p**

where

**λ = 3x 2 1 + a 2y1 mod p**

Let P be any point on the elliptic curve. Multiplication operation over P is defined by the repeated addition. k P = P + P + P +···+ k times.

If x1 = x2 and y1 = y2 = 0 or x1 = x2 and y1 = −y2, the points is said to intersect at infinity denoted by O. Figure 1(c) and 1(d) shows graphical representation of Point at Infinity.

Let us consider an elliptic curve

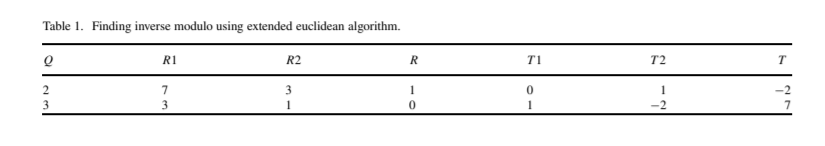
**y2 = x 3 + 2x + 4 mod 7**

It has got the following coordinate points. {O,{0, 2},{0, 5},{1, 0},{2, 3},{2, 4},{3, 3},{3, 4},{6, 1},{6, 6}}. To perform point addition of two points {0, 5} and {3, 4}, we need to find lambda.

**λ = 4 − 5 3 − 0 mod 7**

**λ = −1 3 mod 7**

For finding Inverse Modulo we have used Extended Euclidean Algorithm shown in Table 1.



Where

• Q = Quotient for R1 divided by R2;

• R1 = Modulus value initially, followed by left shift of previous value of R2 in later cases.

• R2 = Denominator value initially, followed by left shift of value from previous R in later cases.

• R = Remainder of R1 divided by R2. • T 1 = 0 initially, followed by left shift of previous value from T2.

• T 2 = 1 initially, followed by right shift of previous value from T . • T = T 1 − Q ∗ T 2. • Continue till R = 0, and inverse modulo is given by the value at T 2.

**λ = −1 ∗ −2 mod 7**

**λ = 2**

Since ECC is a public key cryptography, we require a public key and a private key. Consider Alice and Bob are the two communicating parties. They agree upon a common Elliptic curve equation and a generator G. Let Alice and Bob private keys be n A and nB respectively. Alice and Bob public keys are given by

**Pa = nAG**

**Pb = nBG**

respectively. If Alice want to send a message ‘Pm’ to Bob, Alice uses Bob’s public key to encrypt the message. The cipher text is given by

**Pc = {kG, Pm + k Pb}**

where ‘k’ is a random integer. The random ‘k’ make sure that even for a same message the cipher text generated is different each time. This gives a hard time for someone who is illegally trying to decrypt the message. Bob decrypts the message by subtracting the coordinate of ‘kG’ multiplied by nB from‘Pm + kPb’.

**Pm = {Pm + k Pb − nBkG}**

Here multiplied does not mean simple multiplication that we do in algebra, rather it is multiple addition of points using the point addition method stated above in point multiplication. As the multiplier nB is the secret key of Bob, only Bob can decrypt the message sent by Alice.

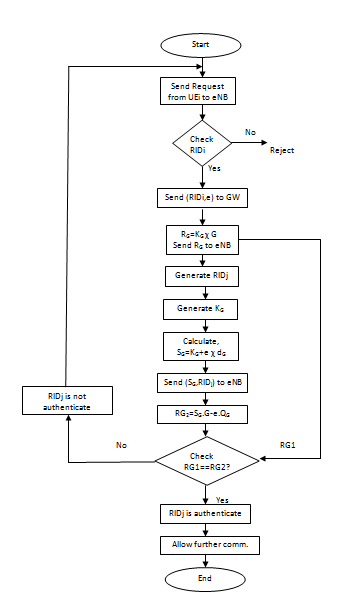
**4.2 Algorithm**

To achieve security between eNB and GW, we consider the implementation of Elliptic Curve Cryptography (ECC). In the conventional SeDS protocol system, to establish secure communication before D2D detection by gateway can be implemented through following steps.

1. Once service request will be sent from UEi to eNB, the authentication will be checked by eNB and RIDi will be sent to GW. Also, one random integer e ϵ [1,n-1] will be selected by eNB. (RIDi, e) will be sent to GW. Where n is the order chosen for ECC operations.
2. Device to device detection will be performed by PSCF in GW. Let the real identity generated for the detected device is RIDj. Also, one random integer key KG ϵ [1,n-1] will be selected by GW. Finally, RG=KGχG will be send to eNB. e and KG for eNB and GW can be considered as temporary secret key so that it helps to hide their real identity.
3. From the random integer selection, GW will calculate one SG parameter. Where, SG= KG + e × dG, + is used for scalar addition and dG is the secret key of GW. From II and III step (SG, RIDj) will be sent to eNB.
4. From received data, eNB will check , RG = SG.G – e.QG where, QG public key of GW. If obtained RG and calculated RG is same, eNB will consider RIDj as the authenticated and in this way the secure communication can be established in between eNB and GW. [10] Once RID will be authenticated, further communication between two user equipments can be carried out using the steps of conventional protocol system. (Refer Fig. 2) [12][13]

The methodology that implemented here is the combination of symmetric cryptography, Public Key Infrastructure and ECC. The proposed idea can be implemented on Network Simulator 3 (NS3) software to verify the simulation results.

**4.3 Flowchart**



**4.4 Overall Code**

* **interface**

clc

clear all

n=input('press 1 to register any other code\npress 2 to send user request\n');

%if pressed 1, a device code is entered to make a new regestry

while(n==1)

code=input('enter the code of the device to be registered\n');

%the code entered will then will be validated by the function

%check(code) in order to check if it has already been registered.

if(check(code)>0)

fprintf("already registered\n");

%if the new code doesnt match with the codes in the database then it new registers the code in device\_database1.txt.

elseif check(code)==0

register(code);

%upon new registry, a real identity number RIDI will be randomly

%generated and is updated in the enb1.txt file. in addition to this

%RIDJ will also be generated and will be updated in the gw1.txt

%file.

end

n=input('press 1 to register any other code\npress 2 to user request\n');

end

%if pressed 2 a user request is sent

while n==2

%the device code has to entered in ordered to check whether it is

%authenticated to do so

code=input('enter the device code');

%if the device is registered and authenticated it proceeds to further

%D2D request approval

if (check(code)>0)

[e]=enb();

[G,dG,Kg,Qg]=gw();

Rg1=(Kg\*G)

Sg=(Kg+(e\*dG))

Rg2=(Sg\*G-e\*Qg)

pause(1);

fprintf("device to device communcation approved for device code %d\n",code);

n=input('press 1 to register any other code\npress 2 to user request\n');

%if the device is not registered and authenticated it propmts the user

%to regiter and get authenticate itself first.

else

fprintf("Please register\n");

end

n=input('press 1 to register any other code\npress 2 to user request\n');

end

* **check.m**

%this function checks the literal in the file bieng passed as an input if it there or not

function y=check(literal)

%opens the file device\_database1.txt

fid=fopen('device\_database1.xlsx');

y=0;

literal=num2str(literal);

tline=fgetl(fid);

while(ischar(tline))

matches=strfind(tline,literal);

num=length(matches);

if num>0

y=y+num;

% fprintf(1,"%d %s\n",num,literal);

end

tline=fgetl(fid);

end

%succesfully closing the file

fclose(fid);

* **enb.m**

function [e]=enb()

e=rand(1,1)\*(14);

% [G,dG,Kg,Qg]=gw();

% Rg1=Kg\*G;

% Sg=Kg+(e\*dG);

* **gw.m**

function [G,dG,Kg,Qg]=gw()

Kg=rand(1,1)\*(14);

G=10;

dG=103;

Qg=147;

% [e,Sg]=enb();

% Rg2=Sg\*G-e\*QG;

* **register.m**

%this function registers a new device code and authenticates it.

function y=register(device\_code)

device\_code=num2str(device\_code);

fid=fopen('device\_database1.xslx','a+t');

fprintf(fid,'%s\n',device\_code);

fclose(fid);

ridi=num2str(round(0.75\*rand(1,8)));

ridj=num2str(round(0.75\*rand(1,8)));

fid=fopen('enb1.xslx','a+t');

fprintf(fid,'%s %s\n',device\_code,ridi);

fclose(fid);

fid=fopen('gw1.xlsx','a+t');

fprintf(fid,'%s %s\n',device\_code,ridj);

fclose(fid);

fprintf("\ndevice code registered\nwaiting for authentication\nplease wait.....\n");

pause(1);

fprintf("please wait..\n");

pause(1);

fprintf("device code has been succesefully authenticated\n");

* **Point Add**

arr=zeros(7,2);

for x=1:7

i=x;

x=x-1;

y1=(x^3+(2\*x)+4);

y=mod(y1,7);

y=round(y^(1/2))

arr(i,1)=x;

arr(i,2)=y;

arr

end

G=zeros(1,2);

p=randi(7)

G(1)=arr(p,1);

G(2)=arr(p,2)

Kg=randi(7)

Rg1=zeros(1,2);

Rg1(1)=G(1);

Rg1(2)=G(2);

for i=1:Kg-1

if Rg1(1)==G(1) && Rg1(2)==G(2)

fprintf('if both the points are same\n');

lam=(3\*(Rg1(1)^2)+2)/(2\*Rg1(2));

x3=mod(((lam^2)-2\*Rg1(1)),7);

y3=mod((lam\*(Rg1(1)-x3)-Rg1(2)),7);

Rg1(1)=x3;

Rg1(2)=y3;

else

fprintf('if both the points are different\n');

lam1=(G(2)-G(1))/(Rg1(2)-Rg1(1));

x4=mod((lam1^2-Rg1(1)-Rg1(2)),7);

y4=mod((lam1\*(Rg1(1)-x4)-Rg1(2)),7);

Rg1(1)=x4;

Rg1(2)=y4;

end

end

fprintf('final Rg1 value\n');

Rg1

e=randi(6);

dg=4;

fprintf('secret key of GW is \n%d\n',dg);

Sg=Kg+(e\*dg)

QG=zeros(1,2);

p1=randi(7)

QG(1)=arr(p1,1);

QG(2)=arr(p1,2);

Rg5=zeros(1,2);

Rg5(1)=G(1);

Rg5(2)=G(2);

Rg6=zeros(1,2);

Rg6(1)=QG(1);

Rg6(2)=QG(2);

for i=1:Sg-1

if Rg5(1)==G(1) && Rg5(2)==G(2)

fprintf('if both the points are same\n');

lam=(3\*(Rg5(1)^2)+2)/(2\*Rg5(2));

x3=mod(((lam^2)-2\*Rg5(1)),7);

y3=mod((lam\*(Rg5(1)-x3)-Rg5(2)),7);

Rg5(1)=x3;

Rg5(2)=y3;

else

fprintf('if both the points are different\n');

lam1=(G(2)-G(1))/(Rg5(2)-Rg5(1));

x4=mod((lam1^2-Rg5(1)-Rg5(2)),7);

y4=mod((lam1\*(Rg5(1)-x4)-Rg5(2)),7);

Rg5(1)=x4;

Rg5(2)=y4;

end

end

for i=1:e-1

if Rg6(1)==QG(1) && Rg6(2)==QG(2)

fprintf('if both the points are same\n');

lam=(3\*(Rg6(1)^2)+2)/(2\*Rg6(2));

x3=mod(((lam^2)-2\*Rg6(1)),7);

y3=mod((lam\*(Rg6(1)-x3)-Rg6(2)),7);

Rg6(1)=x3;

Rg6(2)=y3;

else

fprintf('if both the points are different\n');

lam1=(QG(2)-QG(1))/(Rg6(2)-Rg6(1));

x4=mod((lam1^2-Rg6(1)-Rg6(2)),7);

y4=mod((lam1\*(Rg6(1)-x4)-Rg6(2)),7);

Rg6(1)=x4;

Rg6(2)=y4;

end

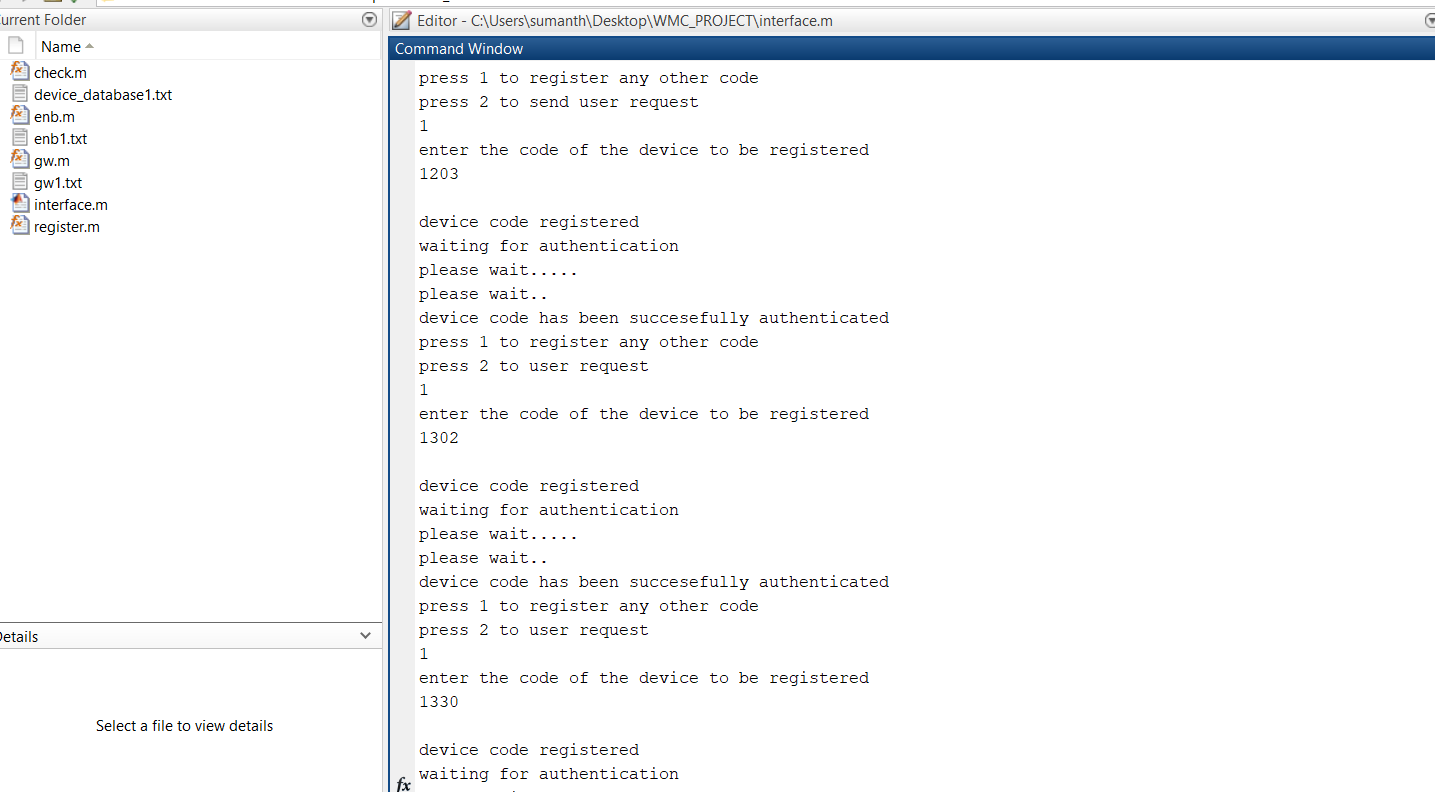
end

fprintf('Rg2 values are\n');

Rg2=Rg5-Rg6

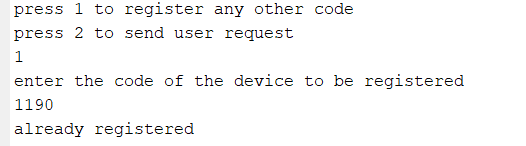
**4.5 Results with Description about figures**

The output after the simulation is shown in figures. The output screenshots are shown in figures 1-6.



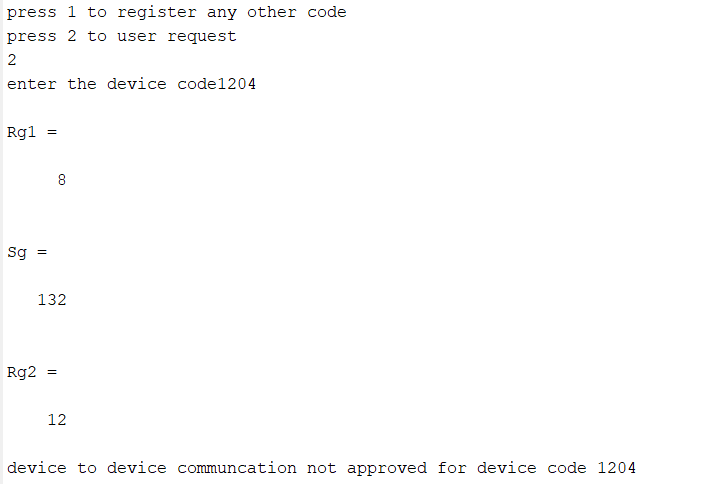
***Figure 1: Output Screenshot***

Above screenshot represent the output of the code ‘register.m’. Here by entering 1 or 2 to register the code, to request user for the values.

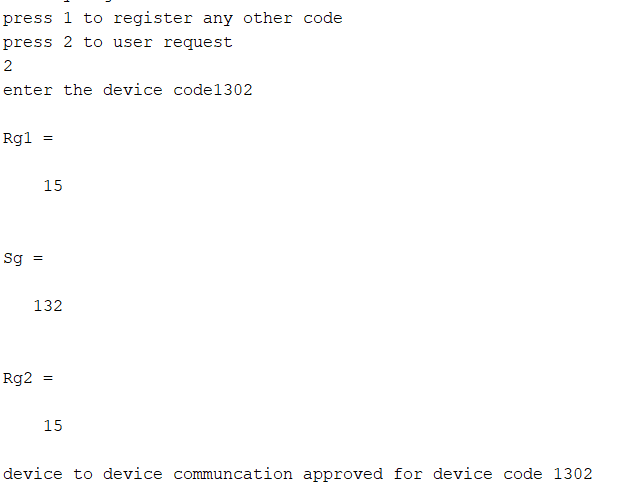


***Figure 2: Output Screenshot***

From above screenshot, If we press the same code to register then the output shows “already registered”.

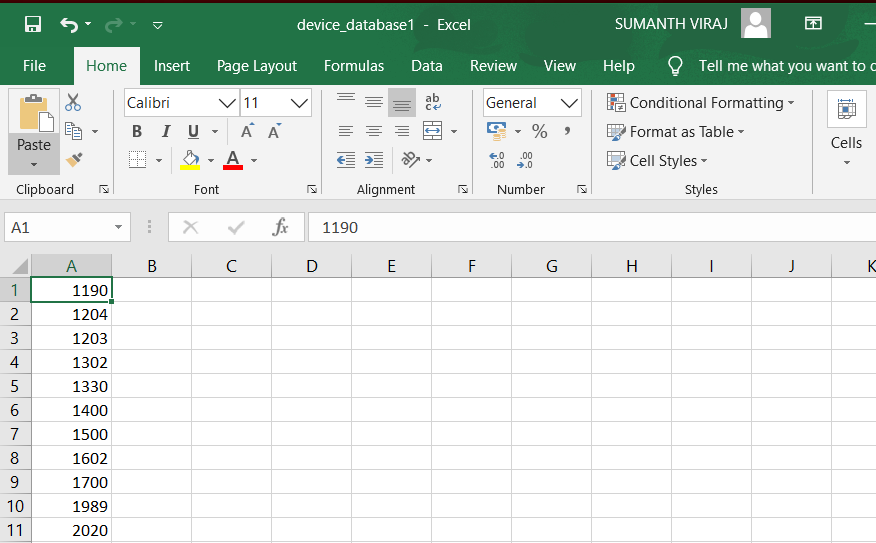


***Figure 3: Output Screenshot***



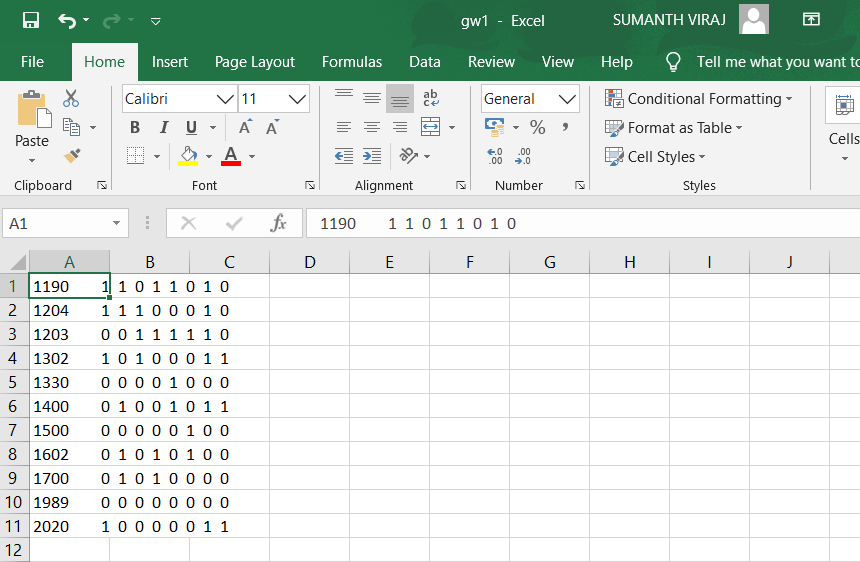
***Figure 4: Output Screenshot***

Above figure 3 & 4, represent the user request values of rg1, rg2 and sg by pressing ‘2’. If both rg1 and rg2 values are equal then device to device communication is approved for the input device code. If both rg1 and rg2 values are not equal, then device to device to communication is not approved for the input device.



Above are the registered codes will be saved in a excel sheet name devie\_database1.

***Figure 5: Output Screenshot***



***Figure 6: Output Screenshot***

In Figure 6, code values will be saved in binary values.

A while loop is initialized to compare rg1 and rg2 values, if both values are equal then RIDj is authenticate and allow further communication. If both the values are not equal then RIDj is not authenticate and again goes to start.

**CHAPTER V**

**CONCLUSION AND FUTURE WORKS**

We have proposed an additional security system in SeDS protocol system to establish secure communication in between eNB and GW for D2D communication in LTE-A network. The system is explicitly design to achieve authenticity in the communication while detecting proper device by the GW. The conventional SeDS protocol was implemented using digital signature and symmetric encryption. Furthermore, we have included ECC so that even security between eNB and GW could not get compromised.

We have analysed the D2D communication scenario and proposed above idea but its validity needs to be checked by implementing simulation on NS3 platform. The limitation to this paper is it needs to be checked whether the idea could get implemented when more than two user equipments are there.

**References**

[1] J. Chen, C. Yang and Y. Mai, "A novel smart forwarding scheme in LTE-Advanced networks", *China Communications*, vol. 12, no. 3, pp. 120-131, 2015.

[2] D. Choi and H. Choi, "An Group-based Security Protocol for Machine Type Communications in LTE-Advanced", Journal of the Korea Institute of Information Security and Cryptology, vol. 23, no. 5, pp. 885-896, 2013.

[3] L. Militano, M. Condoluci, G. Araniti, A. Molinaro and A. Iera, "When D2D communication improves group oriented services in beyond 4G networks", Wireless Netw, vol. 21, no. 4, pp. 1363-1377, 2014.

[4] S. Ramasubramanian, s. chung, S. Ryu and L. Ding, "Secure and Smart Media Sharing Based on a Novel Mobile Device-to-Device Communication Framework with Security and Procedures", ACM, pp. 35-49, 2015.

[5] Z. Aiqing, C. Jianxin, H. Rose and Q. Yi, “SeDS: Secure Data Sharing Strategy for D2D Communication in LTE-Advanced Networks”, IEEE Transaction on Vehicular Technology, Vol.65, No.4, pp. 2659-2672, 2016.

[6] A. Sharma, A. Trivedi and N. Roberts, "Efficient Load Balancing using D2D Communication and Biasing in LTE-Advance Het-Nets", ACM, 2015.

[7] H. Tang, Z. Ding and B. Levy, "Enabling D2D Communications Through Neighbor Discovery in LTE Cellular Networks", IEEE Transactions on Signal Processing, vol. 62, no. 19, pp. 5157-5170, 2014.

[8] R. Lu, X. Lin, and X. Shen, “SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,” IEzaEE Trans. Parallel Distrib. Syst., vol. 24, no. 3, pp. 614–624,Mar. 2013.

[9] M. Mana, M. Feham, and B. Bensaber, “Trust key management scheme for wireless body area networks,” *Int. J. Netw. Security*, vol. 12, no. 2, pp. 75–83, 2011.

[10] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, “Morality-driven data forwarding with privacy preservation in mobile social network,” *IEEE* *Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3209–3222, Sep. 2012.

[11] Y. Hao, J. Tang, and Y. Cheng, “Secure cooperative data downloading in vehicular ad hoc networks,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 523–537, Sep. 2013.

[12] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” in *Proc. Int. Cryptol. Conf.*, 2001, vol. 2139, LNCS, Springer- Verlag, pp. 213–229.

[13] H. Soran, “ Lightweight Security Solutions for LTE/LTE-A Networks”, Networking and Internet Architecture [cs.NI]. Universit\_e Paris Sud - Paris XI, 2014.

[14] Andrew Rukhin, Juan Soto, James Nechvatal, Elaine Barker, Stefan Leigh, Mark Levenson, David Banks, Alan Heckert, James Dray, San Vo, Andrew Rukhin, Juan Soto, Miles Smid, Stefan Leigh, Mark Vangel, Alan Heckert, James Dray, and Lawrence E Bassham Iii. A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2001.

|  |  |  |
| --- | --- | --- |
|  |  |  |

**BIODATA**

Name : A Sumanth



Mobile Number : +91-89 19 23 33 57

E-mail : achari.sumanth2017@vitstudent.ac.in

Permanent Address : VIT University, Chennai

Name : Ayan Nath

Mobile Number: : +91-94 91 80 61 12

E-mail : [ayan.nath2017@vitstudent.ac.in](mailto:ayan.nath2017@vitstudent.ac.in)

Permanent Address : VIT University, Chennai

Name : G PRAVEEN



Mobile Number : +91-73 37 37 32 85

E-mail : galla.praveen2017@vitstudent.ac.in

Permanent Address : VIT University, Chennai