SECURE TUNNELS IN 4G LTE NETWORKS

C.A WEERASINGHE

2017

SECURE TUNNELS IN 4G LTE NETWORKS

A dissertation submitted for the Degree of Master 0f Science in Information Security

CHIRAN ANUPRIYA WEERASINGHE.
University of Colombo School of Computing
2017

Masters Project Final Report
March 2017

Project Title	SECURE TUNNELS IN 4G LTE NETWORKS		
Student Name	CHIRAN ANUPRIYA WEERASINGHE		
Registration No. & Index No.	14770252 2014MIS025		
Supervisor's Name	DR. AJANTHA ATHUKORALA		
Please Circle the appropriate	**Master's Program**	**Type**	
	MIS	**Research**	**Implementation**
For Office Use Only			

Declaration

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute.

To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Students Name:

Signature: Date:

This is to certify that this thesis is based on the work of
Mr. /Ms.
Under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by:

Supervisor Name:

Signature: Date:

ABSTRACT

Mobile networks are moving from traditional voice based service rendering to all IP based data services rendering with high speed data transmission introduced in LTE technology. Ensuring confidentiality of data transmitting in LTE data-plane is still challenge. This dissertation address the question of how securing data transmitting in the LTE network so as to use for the enterprise's VPN. Layer-2 and Layer-3 are VPN technology use by enterprises to connect their branch office with head office. Through this project, implement the system for secured communication between those head offices and branch offices using LTE mobile broad band network. Using LTE mobile network for providing Layer-2 and Layer-3 VPN service is very coast effective way compared to existing technologies. Having mobility and maintenance-free Layer-2 and Layer-3 secure VPN system is implemented in this project.

Setup LTE mobile network with different APN for creating Layer-2 and Layer-3 tunnels. Without doing any modification in eNodeB create Layer-3 tunnels (L3-VPN) to connect geographically separated private LANs through the ISP's public network. Create separate routing instance at LTE core network, isolate the tunnelling data packets from other internet users. Extend the tunnel traffic from LTE core network to ISP MPLS network to merge the tunnel with other wireless technologies like WiMAX. Dedicated virtual routing and forwarding instance creates for each Layer-3 VPN to handle their routing table independently. IPSec protocol use to create secured tunnel with pre-shared security key. Client-server architecture is used to build L2-tunnel (L2-VPN) inside the LTE mobile network without having any changes to eNodeB. Server has placed between PDN-gateway and MPLS edge router while client is placed at L2-tunnel end point. Marked data packet with IEEE dot1q tag from L2-server to MPLS edge, make the flexibility to extend the tunnel with other wireless technologies. Virtual-template creates for particular tunnel separate the users in a particular Layer-2 tunnel. The protocol use to create L2-tunnel is L2TP that wrap the end user's IP packet with L2TP header and send through the LTE network to other end. IPSec protocol suit with the ISAKMP frame work use to exchange pre-shared key for build IPSec secured tunnel inside the L2TP tunnel.

A user in LTE network has two bearers (tunnels) that are signalling bearer and data bearer to have services from ISP. The signalling bearer has encrypted all the way it going through. But data bearer is encrypted up to eNodeB from the LTE wireless router. So the intruder who can capture the data bearer in between eNodeB and PDN-gateway can read the data. Layer-2 and Layer-3 Packet captured at PDN-gateway clearly shows the information inside the data packets. After creating encrypted Layer-2 and Layer-3 tunnels, packet captured at PDN gate way does not show any information inside it. IPSec protocol encrypt the information inside the data packet with Pre-shared key agreed by all parties in the particular communication channel. Again there are many boundaries to overcome for capture the LTE data bearer. Therefore security in LTE network for day-to-day internet users are in satisfied level. But for the enterprises who connect their offices through VPN in LTE need extra layer of security to ensure their information is not at the risk when they using Layer-2 or Layer-3 VPN system proposed by this project. IPsec tunnel inside the L2 and L3 tunnel (VPN) make secure communication over LTE networks providing extra layer of security by encrypting the IP packet payload.

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all who support me to complete this thesis. Especially thankful to my project supervisor Dr. Ajantha Athukorala for the continuous support given me throughout the project.

I would like to thank all my friends and colleges at my work place for support given me to success this project.

This thesis would not have been possible unless the support of my family. I specially thankful to them.

Chiran weerasinghe

08th March 2017

Table of Contents

LIST OF FIGURES AND TABLES

ABBREVIATIONS

LTE – Long term evolution
4G – 4th Generation
ADSL – Asymmetric digital subscriber line
WiMAX – Worldwide Interoperability for Microwave Access
VPN – virtual private network
IPSec – Internet Protocol Security
MPLS – Multiprotocol Label Switching
EPC - Evolved Packet Core
GTP-U – GPRS tunnelling protocol-user plane
GPRS – General packet radio service
GRE – Generic routing encapsulation
S-GW – Serving-gateway
P-GW – PDN-gateway
PDN - Packet date network
EMM – EPS mobility management
ESM – EPS session management
MME – Mobility management entity
RRC – Radio resource controller
HSS – Home subscriber sub-system
GTP-C – GPRS tunnelling protocol-control plane
PMIP – Proxy mobile IPV6
ISP – Internet service provider
OSI – Open system interconnection
IP – Internet protocol
L2TP – Layer-2 tunnelling protocol
PDCP – Packet Data Convergence Protocol
RLC – Radio Link Control
ROHC – Robust header compression
NAS – Non access stratum
S-TMSI – SAE-Temporary Mobile Subscriber Identity
UMTS - Universal Mobile Telecommunications Service

CHAPTER 1: INTRODUCTION

1.1 PROJECT INTRODUCTION

In this project, traditional 4G LTE network which is used for mobile (voice) and data (broadband) communication has re-architectured to create secured Layer-3 (GRE) tunnels and Layer-2 (L2TP) tunnels over the 4G LTE networks make private communication channel for larger enterprises to connect their geographically separated systems through the fastest mobile communication technology which has less power consuming, less space consuming, maintenance free and very cost effective system compare to other technologies like fiber, ADSL and WiMAX. Implemented system in this project operate in same frequency range as 4G LTE operate that save the frequency for Internet service providers. The existing solution like WiMAX operate in separate frequency band other than LTE to deliver the L2-tunneling and L3-tunneling services. Delivering the voice, internet, L2-tunnelling (L2-VPN) and L3-tunnelling (L3-VPN) using single mobile access network technology save lot of money for ISPs.

1.2 GOAL OF THE PROJECT

The project primary goal is to create secured Layer-2 and Layer-3, point-to-point and point to multi-point tunnels over the 4G LTE network.

1.3 SCOPE OF THE PROJECT

Create Layer-3 tunnel over LTE network wrapping data packet using GRE which is most popular tunnelling technology available in the routers. Create IPSec tunnel inside the L-3 tunnel secure data transfer. Create Layer-2 tunnel over LTE network wrapping data packets using L2TP and create IPSec tunnel inside L2-tunnel for secure data transfer.

1.4 OVERVIEW OF THE REPORT

Chapter two discuss the existing literature related to the project that include brief introduction to LTE, its security vulnerabilities and available tunnelling solutions. In chapter three discuss the design of secured L2 and L3 tunnels over LTE. In chapter four discuss the implementation carried out to create secured L2 and L3 tunnel in the LTE network and MPLS network. In chapter five analyse the results that have taken before and after the secure tunnel creation. In chapter six conclude the decision that have taken based on the analysis carried out in chapter five and the future expansion for the project.

CHAPTER 2: LITRETURE REVIEW

2.1 4G LTE NETWORK ARCHITECTURE

4th generation Long term Evolution (4G LTE) is the newest technology in the wireless cellular networks which provides high speed data connective for both residential and co-operate users. So it is important to ensure the security of the date going through the networks. In LTE network architecture itself has two tunnels which use for data traffic and signalling traffic. The following diagrams show that the architecture of the 4G LTE network.

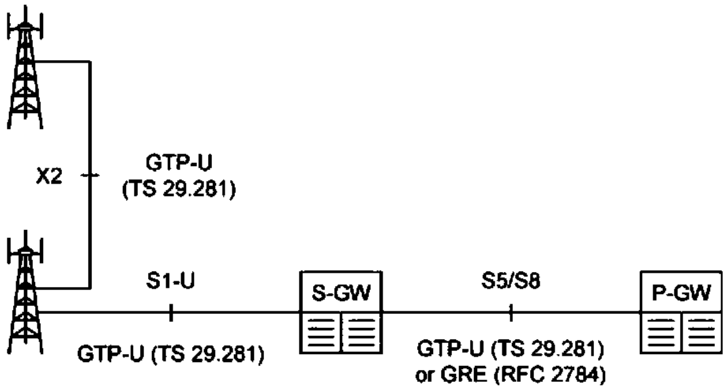

Figure 1: Data tunnel connectivity [1]

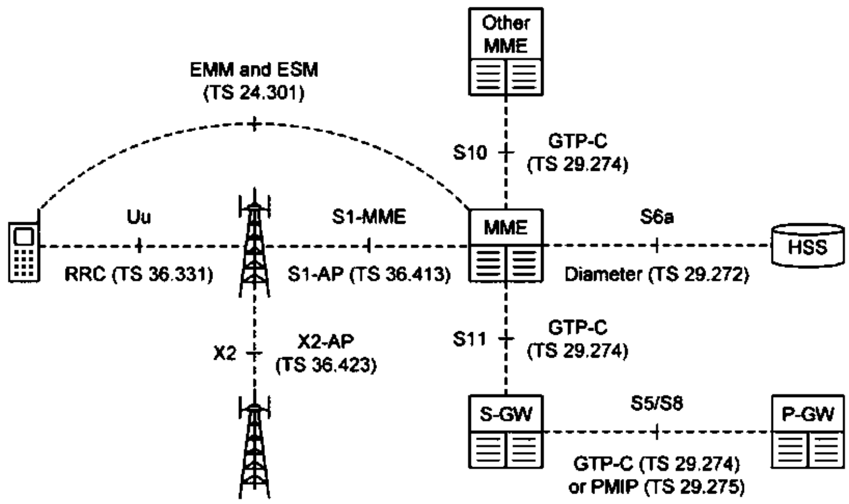

Figure 2: Signalling tunnel connectivity [1]

P-GW is the tunnel end point for both signalling and data traffic in the 4G LTE network. For each user connected to the LTE network has his own tunnel. This project is to identify how these tunnels are bind together to make point to point tunnel or point to multi-point tunnels. Further these tunnels could be layer 2 (Data link layer) or layer 3 (Network layer) tunnels.

At the tunnel end point on P-GW it is possible to capture the data in plane text and can rebuild the transmitted data. Overcome this issue this project is to identify the encryption mechanism, thus it is very difficult to decrypt the data without key.

2.2 E-UTRAN USER PLANE

An IP packet for a UE is encapsulated in an EPC-specific protocol and tunnelled between the P-GW and the eNodeB for transmission to the UE. Different tunnelling protocols are used across different interfaces. A 3GPP-specific tunnelling protocol called the GPRS Tunnelling Protocol (GTP) is used over the S1 and S5/S8 interfaces. The E-UTRAN user plane protocol stack shown in below Figure consisting of the Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC) and Medium Access Control (MAC) sublayers that are terminated in the eNodeB on the network side [2].

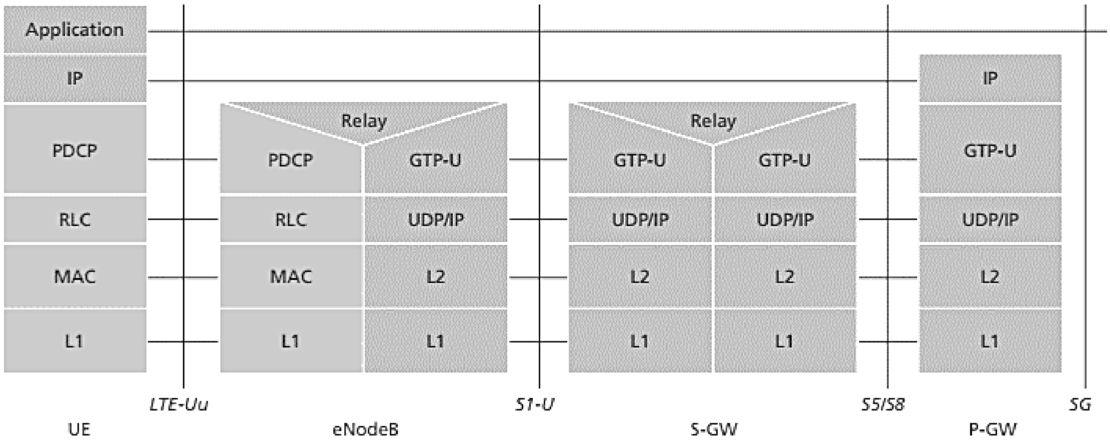

Figure 3: User plane protocol stack [2]

2.3 E-UTRAN CONTROL PLANE

The protocol stack for the control plane between the UE and MME is shown in below. The lower layers perform the same functions as for the user plane with the exception that there is no header compression function for the control Plane. The Radio Resource Control (RRC) protocol is known as "layer 3" in the access stratum protocol stack. It is the main controlling function in the access stratum, being responsible for establishing the radio bearers and configuring all the lower layers using RRC signalling between the eNodeB and the UE [7].

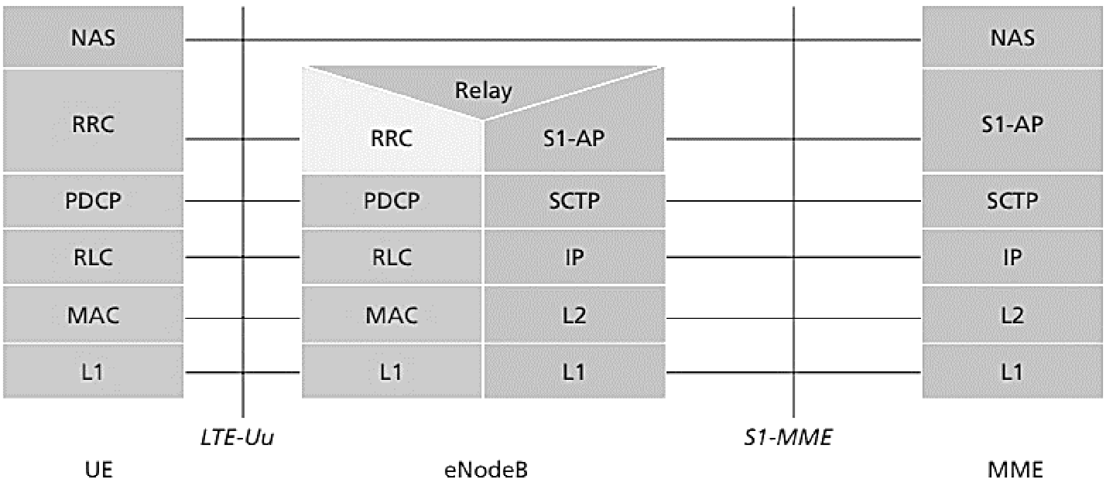

Figure 4: Control plane protocol stack [2]

2.4 PACKET DATA CONVERGENCE PROTOCOL (PDCP)

PDCP sublayer is part of the LTE layer 2 protocols, which is responsible for the IP header compression of user-plane data packets in order to reduce the number of information bits transmitted over the air-interface. The header compression mechanism is based on the Internet Engineering Task Force (IETF) standard robust header compression (ROHC). PDCP sublayer is also responsible for ciphering and integrity protection of control-plane RRC messages, as well as in-sequence delivery and duplicate removal [3].

At the receiver side, the PDCP perform the corresponding deciphering and decompression operations. There is one PDCP entity per radio bearer (RB) configured for a terminal. More specifically, the PDCP sublayer provides the following services to other protocol layers on the user-plane: header compression and decompression using ROHC protocol, transfer of user data, in-sequence delivery of upper layer PDUs at PDCP reestablishment procedure for RLC acknowledged mode (AM), duplicate detection of lower-layer service data units (SDUs) at PDCP reestablishment procedure for RLC AM, ciphering and deciphering and time based SDU discarding in the uplink. The main services and functions of the PDCP on the control-plane include ciphering and integrity protection as well as transfer of control plane data [3].

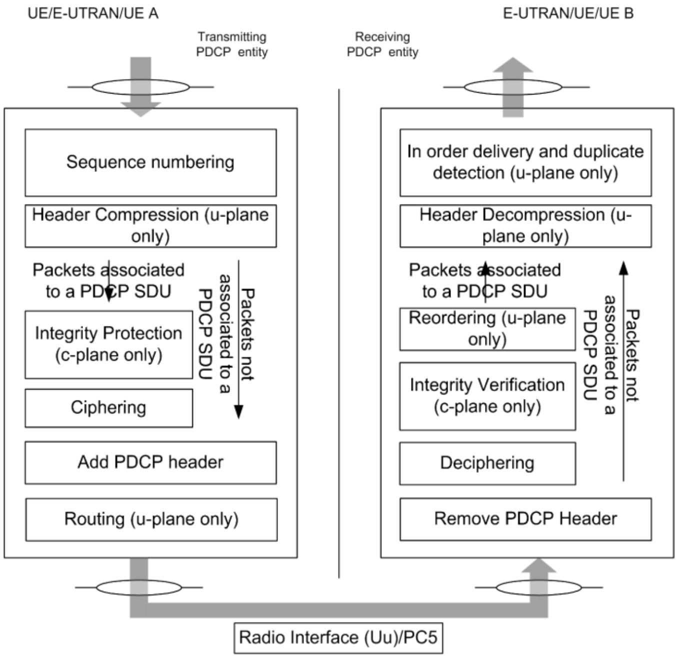

Figure 5: PDCP layer, functional view [4]

2.5 KEY HIERARCHY IN LTE

Network access security is based on a hierarchy of keys that relies on the shared knowledge of a user-specific key, K, which is securely stored in the home subscriber server (HSS) and securely distributed within the universal integrated circuit card (UICC) [1]. The key K is unique for the IMSI which has in stored in the SIM card.

The HSS and UICC derive two keys that are CK and IK from K. Then CK and IK use to derive K_{asme} (access security management entity) key. Mobile equipment and MME use K_{asme} to derive K_{NASenc}, K_{NASint} and K_{eNB} keys. Non access stratum (NAS) signalling messages between mobile and MME use K_{NASenc}, and K_{NASint} for ciphering and integrity protection. MME send K_{eNB} to eNodeB for generating another three keys that are K_{UPenc}, K_{RRCenc} and K_{RRCint}. These are respectively used for ciphering of data, ciphering of RRC signalling messages and integrity protection of RRC signalling messages in the access stratum (AS).

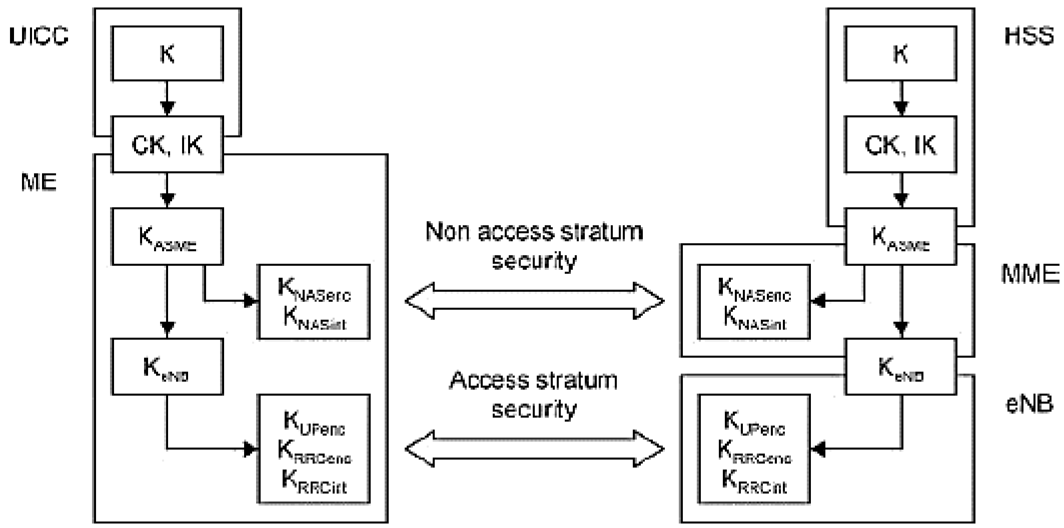

Figure 6: key hierarchy in LTE

K, CK and IK contain 128 bits each and all other keys contain 256 bits. When mobile device detach from the network, IK and CK store in its UICC and MME store K_{asme}. This allows the system to secure the mobile's attach request when it next switches on. Key hierarchy ensures that the AS and NAS keys are cryptographically separate that make knowledge of one set of keys does not help an intruder to derive the other.

2.6 AUTHENTICATION, ENCRYPTION, DECRYPTION, IN LTE

Network access security protects the communications of mobile device with the network, across the air interface which is the most vulnerable area of the LTE architecture using authentication, confidentiality, encryption and decryption. During authentication, the network and mobile confirm each other's identities. The evolved packet core (EPC) confirms that the user is authorized to use the network's services and is not using a cloned device. Similarly, the mobile confirms that the network is genuine and is not a spoof network set up to steal the user's personal data [1].

Confidentiality protects the user's identity. The international mobile subscriber identity (IMSI) is one of the quantities that an intruder needs to clone a mobile, so LTE avoids broadcasting it across the air interface wherever possible. Instead, the network identifies the user by means of temporary identities. If the EPC knows the MME pool area that the mobile is in (for example, during paging), then it uses the 40 bit S-TMSI. Otherwise it uses the longer GUTI. Similarly, the radio access network uses the radio network temporary identifiers (RNTIs) [1].
Ciphering, also known as encryption, ensures that intruders cannot read the data and signalling messages that the mobile and network exchange. Integrity protection detects any attempt by an intruder to replay or modify signalling messages. It protects the system against problems such

as man-in-the-middle attacks, in which an intruder intercepts a sequence of signalling messages and modifies and re-transmits them, in an attempt to take control of the mobile.

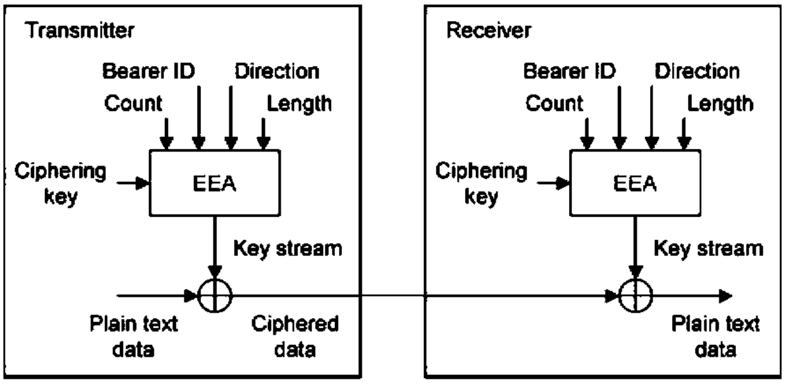

Figure 7: Encryption and decryption [1]

LTE implements ciphering and integrity in the non-access stratum and access stratum to protect EPS mobility and session management messages between the mobile and the MME. This brings two main advantages. In a wide-area network, it provides two cryptographically separate levels of encryption, so that even if an intruder breaks one level of security, the information is still secured on the other [5].

2.7 CRYPTOGRAPHIC ALGORITHMS USE IN LTE

KASUMI ALGORITHM

The first ciphering algorithm for the LTE standard, the Kasumi algorithm, is mainly a block cipher algorithm that uses a key size of 128 bits. The algorithm utilizes two mapping functions to produce the cipher-text, which are called S-boxes. Kasumi was specifically designed as a building block for the UMTS encryption algorithms (UEA1) and integrity algorithms (UIA1) [5].

SNOW 3G ALGORITHM

SNOW 3G was designed as a second cryptographic solution in response to the appearance of newer forms of attacks—algebraic attacks—that would decrease Kasumi-based algorithms' security. Similar to the case of Kasumi, some changes were made to the original SNOW 2.0 to adapt it to the requirements of the demanding 3G environment and defend itself successfully against the newly discovered algebraic attacks. SNOW 3G is used as the core component of both UEA2 and UIA2 [5].

MILENAGE ALGORITHM

The Milenage encryption algorithm is the third 3G security algorithm deployed in LTE that uses a core function of a block cipher in which both block size and key size are 128 bits. Here, we can use the basic form of the Advanced Encryption Standard encryption algorithm as the core function [6].

ZUC ALGORITHM

In addition to the previous 3G cryptographic algorithms, the ETSI SAGE task force, together with Chinese cryptography experts, have already started the design work for a third algorithm pair specifically for 4G security. 128-EEA3 is the LTE encryption algorithm defined straightforwardly using ZUC while 128-EIA3 is the LTE integrity algorithm, designed as a Universal Hash Function using ZUC as its core.

2.8 SECURITY ISSUES IN LTE NETWORKS

In a change from 2G/3G security specifications, 3GPP defined that for LTE all radio network layers between the user equipment (UE) and eNodeB must be protected using the Packet Data Convergence Protocol (PDCP) layer terminated into the eNodeB. However, the control plane between the eNodeB and the MME and the user plane between the eNodeB and the serving gateway are unprotected. Actually, only the control plane between user equipment and the MME (NAS signalling) is protected. Due to this lack of protection on the mobile traffic going through the mobile backhaul network, 3GPP proposed an option to add protection to the S1 and X2 interfaces and the management plane using IPsec, especially when the eNodeB is set up in untrusted locations. IPsec provides a comprehensive set of security features (data origin authentication, encryption, integrity protection) to address these security issues and is defined in the context of the 3GPP security architecture for LTE [7].

2.9 LIMITATIONS OF L7 TUNNELING SOLUTIONS IN LTE

Traditional LTE systems are mobile voice and data networks. SIM card insert to the mobile device allows access to the network that SIM card belong. Software based tunnelling solution are using in these environments and work on application layer of the OSI seven layer model. These software based tunnelling systems use internet connection to connect to the sever which has hosted in internet. User who has access to the tunnel get access to the internet automatically, this is the main drawback of software type tunnelling solutions.

Port forwarding is technique that connect two geographically separated site through LTE technology and it required public IP address for each site and everyone in the internet have access to the site. Only available authentication mechanism is to have user name and password prior to access the device which means that user device is open to attacks like Denial of Service (DoS) and Dictionary. Furthermore, to have a public IP address need to pay extra bill for the service provider.

2.10 GRE TUNNELING PROTOCOL

GRE is a tunnelling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point to point link between routers over an IP networks. GRE allows wide variety of passenger protocols to be transported over the IP network. The main benefit of the GRE tunnel is that it supports IP multicast and therefore is appropriate for tunnelling routing protocols. Traffic that is sent through the GRE tunnel is not encrypted and so susceptible to man in the middle attacks [8]. The below figure shows the structure of GRE packet header.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

C	R	K	S	s	Recurl	Flags	Ver	Protocol Type
Checksum (Optional)								Offset (Optional)
Key (Optional)								
Sequence Number (Optional)								
Routing (Optional)								

Figure 8 : GRE Packet header structure [9]

2.11 LAYER 2 TUNNELING PROTOCOL (L2TP)

L2TP is a protocol that is used to tunnel point to point protocol over a public network using IP. This protocol allows for the encapsulation of any Layer 3 protocol in its packets because of the fact that the tunnelling occurs on Layer 2, thereby making things transparent to Layer 3 and above. UDP is used as the carrier of all L2TP traffic in IP backbone. L2TP does not provide encryption mechanism for the traffic it tunnels [10]. The below figure shows the structure of L2TP packet.

											12	16	32 bit
T	L	X	X	S	X	O	P	X	X	X	X	VER	Length
Tunnel ID													Session ID
Ns (opt)													Nr (opt)
Offset size (opt)													Offset pad (opt)

Figure 9 : L2TP packet structure [11]

2.12 GPRS TUNNELLING PROTOCOL (GTP)

The GPRS Tunnelling Protocol (GTP) is the tunnelling protocol defined by the 3GPP standards to carry General Packet Radio Service (GPRS) within 3G/4G networks. GTP is used to establish a GTP tunnel, for user equipment, between a Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW), and an S-GW and Mobility Management Entity (MME). A GTP tunnel is a channel between two GPRS support nodes through which two hosts exchange data. The S-GW receives packets from the user equipment and encapsulates them within a GTP header before forwarding them to the P-GW through the GTP tunnel. When the P-GW receives the packets, it decapsulates them and forwards them to the external host [12]. The below figure show the GTP header.

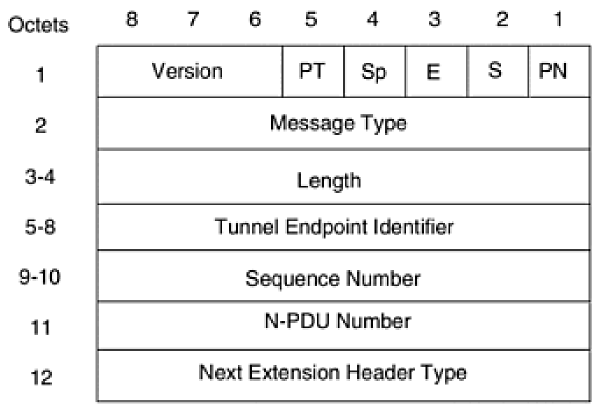

Figure 10 : GTP header [13]

2.13 INTERNET PROTOCOL SECURITY (IPSEC)

IPSec is protocol suit developed by IETF for secure communication in interne and facilitate for interoperable, cryptographically based security. IPSec provides set of security services including access control, protection against replays, connectionless integrity, confidentiality (encryption), limited traffic flow confidentiality and data origin authentication. These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

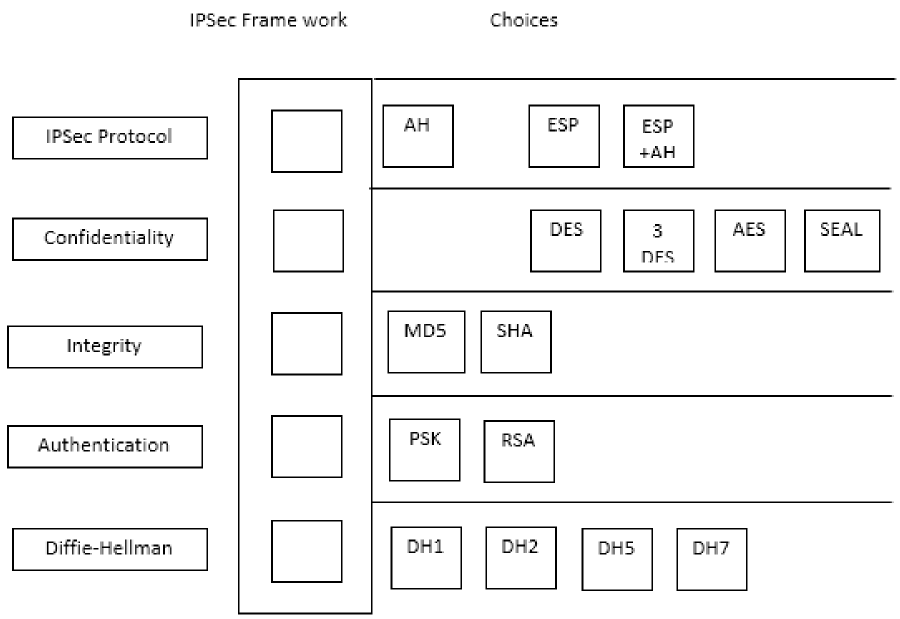

Figure 11 : IPSec frame work

IPSec protocol has two choices that are authentication header (AH) and encapsulation security payload (ESP) or authentication header with encapsulation security payload (AH+ESP). Confidentiality is achieved by using encryption methods that are data encryption standard (DES), triple DES (3DES), advanced encryption standard (AES) and software-optimized encryption algorithm (SEAL). Integrity is achieved by using MD5 and SHA hashing methods. RSA use to ensure authenticity of the information inside IPSec by generating cryptographic keys while PSK share the key manually with users. Securely exchange the keys Diffie–Hellman key exchange (DH1, DH2, DH5, DH7) available in the IPSec frame work.

2.14 ISAKMP

Internet Security Association and Key Management Protocol (ISAKMP) provide frame work to negotiate point-to-point security association (SA), exchange key and authentication data between two parties [14]. Internet key exchange (IKE) which is automated key exchange mechanism use to create SA, implements Oakley Key Determination Protocol (OAKLEY) and Secure Key Exchange Mechanism (SKEME) key exchange inside ISAKMP framework. ISAKMP has define two message types that phase-1 (Main mode) and Phase-2 (Quick mode) for exchanging keys and it not define any key exchange algorithm.

Phase-1 has two modes that are main mode and aggressive mode. The main mode is more secure and gives stronger authentication mechanism, requires six messages exchange between initiator and responder. The aggressive mode require three messages between initiator and responder. Phase-2 has only one mode (quick-mode) that require three message exchange. From master key in the phase-1 derive all other subsequent keys and establish the protection channel while phase-2 establish the IPSec SA and exchange new keys. The below figure show the protocol header of ISAKMP.

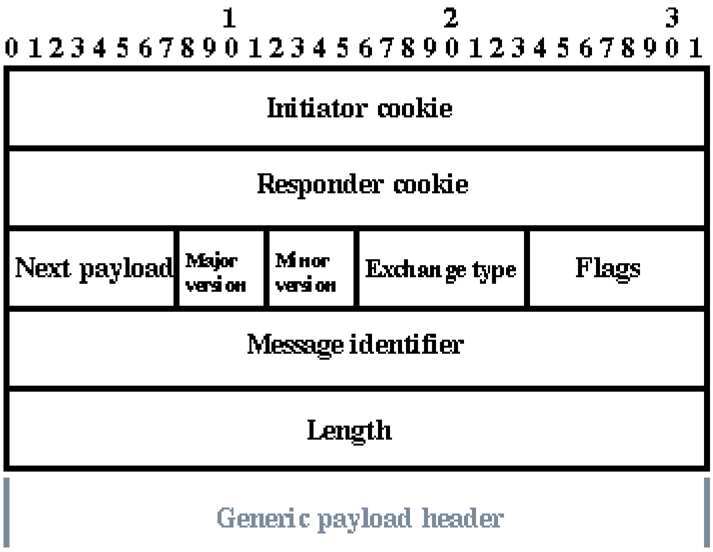

Figure 12 : ISAKMP Protocol header [15]

2.15 RELATED RESEARCH

Most of the researches carried out for securing data in LTE network are focused on introducing more secured key for LTE signalling plane. Data plane still not secure enough for using as to transfer very sensitive data. IPsec protocol suit has identified to secure the LTE network. Implementing IPSec protocol suit in each and every LTE device is a another method found through the researches for securing the data, need higher processing power and it make LTE equipment very expensive.

CHAPTER 3: DESGIN OF SOLUTION

3.1 DESGIN APPROACH

Two types of secure tunnels are create in this project include Layer-2 secure tunnel and Layer-3 secure tunnel. First milestone is to setup LTE network successfully. Top of the LTE network create unencrypted Layer-2 and Layer-3 tunnel. Capture data transmitting through the unencrypted tunnel. Use the same procedure as above and create encrypted tunnel with IPSec and capture the transmitting data through the tunnel for testing and analysis.

3.2 DESGIN ASSUMPTION

Assume Pre-shared key used in IPSec encryption is known by each and every party use the Layer-2 or Layer-3 tunnel. Assume there is no communication between LTE WAN IPs, and third party do not have access to the devices at customer premises.

3.3 OVERALL ARCHITECTURE

Tunnel port facing to the enterprise network take all data traffic coming to the tunnel and deliver to the other end of the tunnel. This architecture mainly has three sections which are enterprise network, LTE access network and LTE core network that are shown in below diagram. The facing interface of the enterprise-network to LTE access router has capability of running IPSec protocol and it encrypt the outgoing date from the router and decrypt the incoming data to the route and create encrypted tunnel.

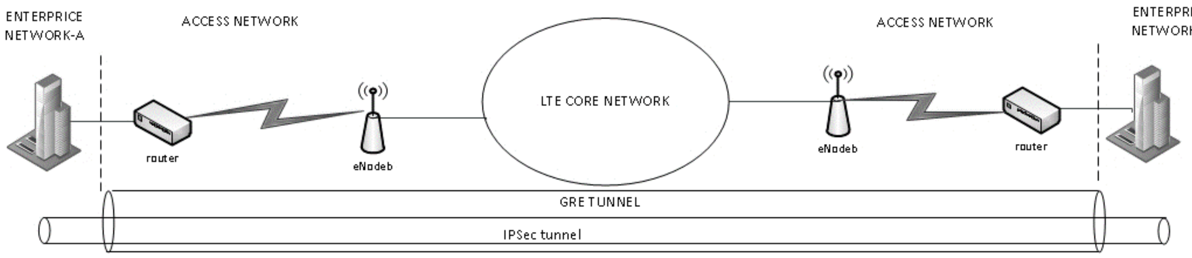

Figure 13 : Over view of tunnel architecture

Generic routing encapsulation (GRE) tunnel create across the LTE core network make the end devise at the tunnel end points to see each other. End devices at tunnel end points does not know about devices in the middle of the architecture. Internet security association and key management protocol (ISAKMP) used in this system and use pre-shared key authentication. Other authentication mechanisms like RSA-Sig and RSA-Encr also possible along with this architecture but for the simplicity of the system this project use the pre-shared key authentication method. AES-256 Encryption algorithm used here and AES-192, AES-128, 3DES and DES are other available encryption algorithms depending on the device at tunnel end points.

3.4 DESGINE OF LAYER-3 TUNNEL

Every connected party to the tunnel has different LAN network and each network has ability to communicate with each other. A common virtual routing instance at MPLS edge use for aggregate different LAN networks. GRE tunnel prior to the IPSec tunnel, create and aggregate using virtual routing instance.

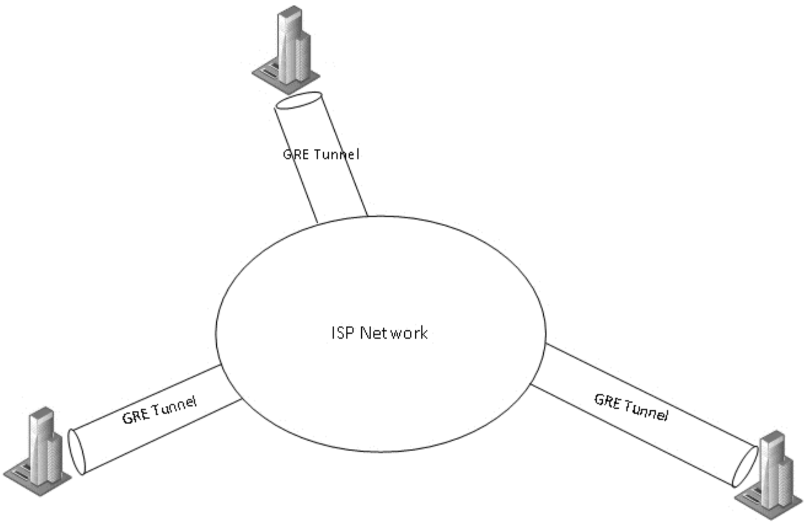

Figure 14 : Design of Layer-3 (GRE) tunnel

Above figure shows the over view architecture of the GRE tunnel create for connecting enterprice networks. Enterprice networks connecting through same GRE tunnel can communicate with each other. Users at tunnel end point do not see any network element in service provider network.

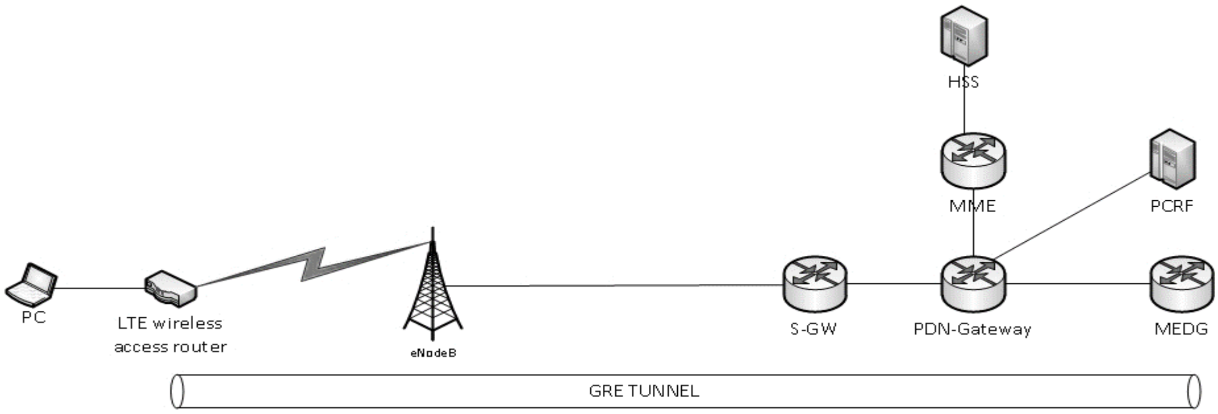

Figure 15 : Network topology of Layer-3 (GRE) tunnel

Layer 3 tunnels impliment in simulation model using Generic Routing Encapsulation(GRE) and connecting those tunnels to PGW in the LTE EPC through the Uu interface. In the PGW separate routing instance need to create to keep route table separately and Access point name (APN) need to be separate so as to keep the tunnel separetely.

3.5 DESGINE OF LAYER-2 TUNNEL

The below figure shows only one side of the symmetric connectivity of L2-Tunnel. From the L2TP server tunnel extend to the other end. Design for Point-to-point L2-Tunnel and point-to-multipoint L2-Tunnel are same. LTE wireless router has SIM card specially programme for L2-Tunnel and L2-Roter also need to programme for the tunnel. IP packets which has tunnel information must have prioritized delivery in LTE network to ensure uninterrupted service for connecting devices through L2-Tunnel.

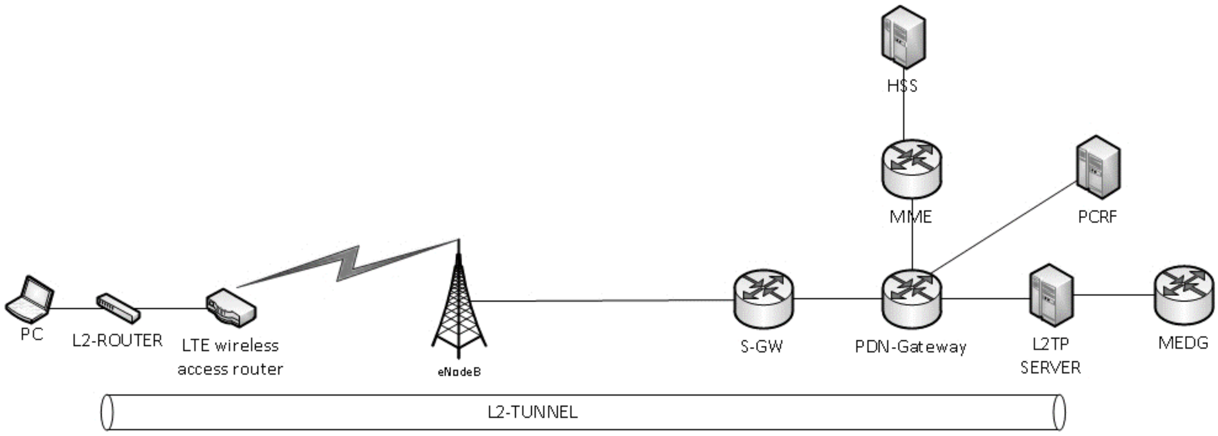

Figure 16 : Network topology of Layer-2 (L2TP) tunnel

3.6 DESGIN OF IPSEC TUNNEL FOR L2/L3

Architecture of IPSec tunnel inside GRE tunnel and L2TP tunnel are same. In network view of point there are few differences. In IPSec and GRE environment have more overhead bits on IP packets than IPSec and L2. The reason is more intermediate networks contribute for creating GRE tunnels. Hashing method use for IPSec tunnel is MD5 and SHA also available. Both Pre-shard key and RSA authentication methods are available and Pre-shared key authentication use for IPSec tunnel creation. Below figure shows the overall architecture of the Layer-2 tunnel.

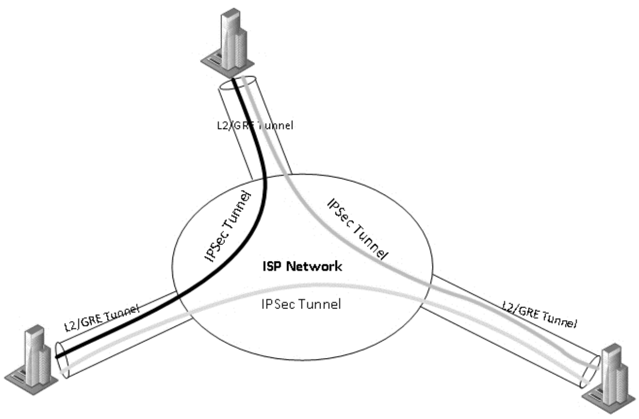

Figure 17 : Desgin view of IPSec tunnel

Below two diagrams respectively shows the Network topology of IPSec tunnel inside L3 tunnel and Network topology of IPSec tunnel over L2-tunnel. IPSec in Layer-3 model, each customer end router authenticate pre-shared key through the GRE tunnel. IPSec in Layer-2 model each customer end router authenticate pre-shared key through the L2TP tunnel.

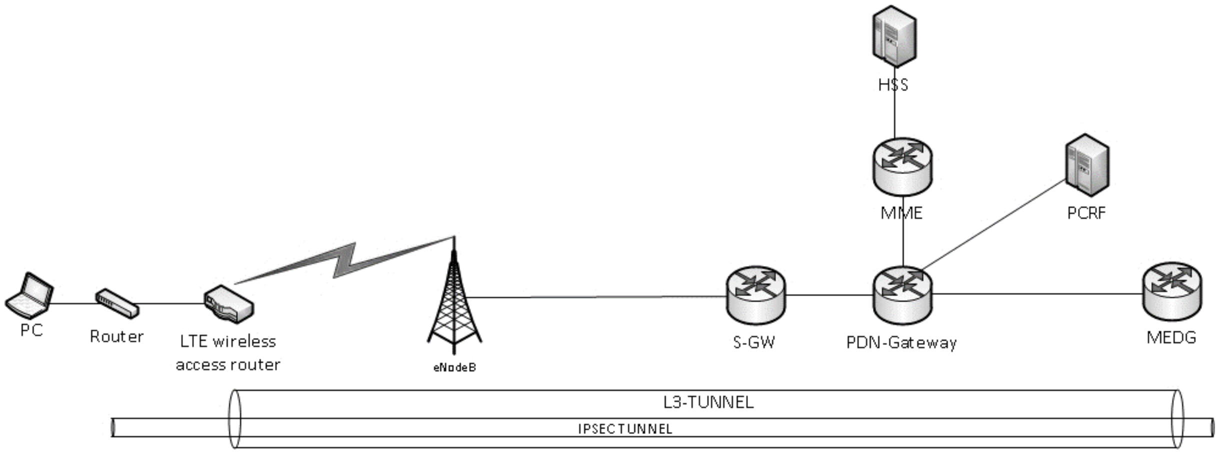

Figure 18 : Network topology of IPSec tunnel inside L3 tunnel

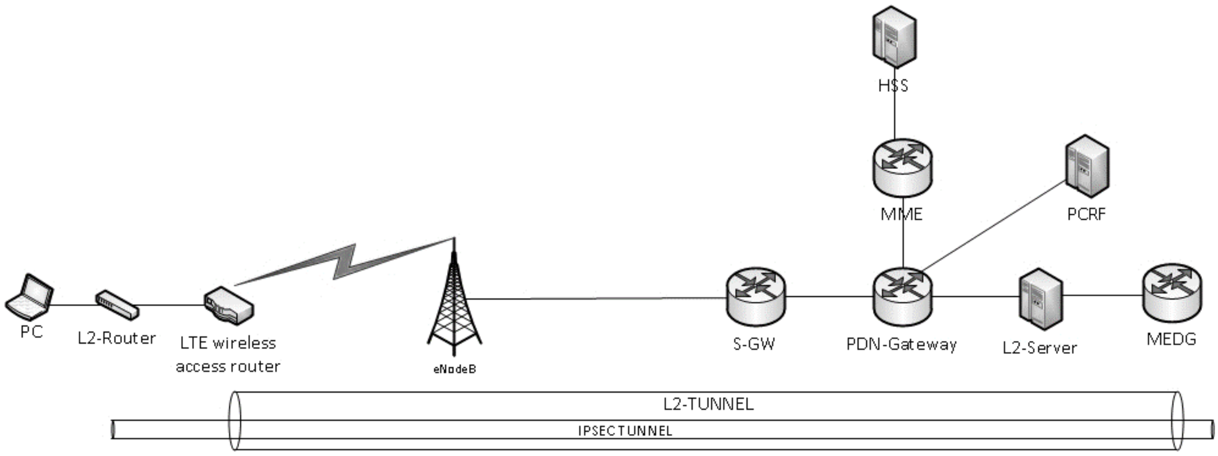

Figure 19 : Network topology of IPSec tunnel over L2-tunnel

3.7 TESTING PROCEDURE

Capture the tunnel traffic without IPSec tunnel in the first attempts to show the information inside the Layer-2 and Layer-3 tunnels are readable. The captured data analyse using Wireshark tool to justify the readability of information transmit over the tunnel. In next stage create the IPSec tunnel inside the L2 and L3 tunnels to transmit encrypted data. Capture the IPSec tunnel traffic to show encrypted information inside the tunnel using Wireshark tool.

CHAPTER 4: IMPLEMENTATION

4.1 TECHNOLOGY CHOISES

Layer-7 VPN is a solution for secure data transmission over LTE network. Limitations in Layer-7 VPNs are, it need to install on every computer. Layer-7 VPN software cannot install in router to connect to the network. GRE protocol use for creating Layer-3 tunnel and L2TP protocol use for creating Layer-2 tunnel.

4.2 LTE CORE NETWORK FOR L3-TUNNEL

Configuration of LTE core network for facilitating GRE tunnel include Home subscriber sub system (HSS), Mobility management entity (MME), PDN-gateway (P-GW) and Policy and charging rule function (PCRF).

HSS configuration include creating separate Access Point Name (APN) template which is integer-character value without spaces between each character and should be similar to the APN created in the PGW. SIM card should have static IP address for communication with SIM card at other end. IP address belong to the same APN can only communicate with each other. For LTE data bearer, quality of service class id (QOSCID) 6 has used which has 300ms packet delay budget and 10^{-6} packet error loss rate. LTE data bearer need to have more prioritise service to keep GRE and IPSec tunnel inside that data bearer. Below code show only the APN creation in the HSS and other configuration in HSS has mentioned in Appendix: A.

```
PGW    #099025
%%LST APNTPL: HLRSN=1, TPLID=605;%%
RETCODE = 0 SUCCESS0001:Operation is successful

                         HLRSN = 1
                         TPLID = 605
                       TPLNAME = 4gvpn
                           APN = 4gvpn
                PDNGWALLOCTYPE = DYNAMIC

Total count = 5

There is together 1 report

---    END
```

The S-GW, P-GW, or MME needs to be selected and the IP addresses of these LTE nodes need to be resolved during attach and PDN connection setup. Adding Name authority pointer (NAPTR) record in the running DNS server inside the MME resolve the IP address of the S-GW, P-GW or MME by creating fully qualified domain name (FQDN).

```
 %%LST DNSN: FQDN="4GVPN.APN.EPC.MNC004.MCC413.3GPPNETWORK.ORG";%%

RETCODE = 0  Operation succeeded

The result is as follows:
-------------------------
           FQDN  =  4GVPN.APN.EPC.MNC004.MCC413.3GPPNETWORK.ORG
Host Name Index  =  101
         Entity  =  PGW
```

```
 Interface Type  =  S5
    S5 Protocol  =  GTP
    S8 Protocol  =  GTP
       Priority  =  0
         Weight  =  100
    Description  =  NULL
(Number of results = 1)

---    END
```

Creating VPN-instance in the PDN-gateway separate the routing table of the APN/APNs that belong to from other routing tables, allowing handle its traffic more flexible way.

```
ip vpn-instance 4gvpn
 description ***4GVPN***
 ipv4-family
  route-distinguisher 605:1
```

Static IP pool define in the PDN-gateway allows HSS to pick an IP address from that pool for subscriber's SIM card when registering to the network. This IP address use as the destination IP address of the GRE tunnel at the MPLS edge router. Creating APN in the PDN gateway link VPN-instance and address pool with APN that allows SIM card which has defined in the HSS to register on network and APN has configured to communicate with PCRF that record the data usage of the SIM card user. The configuration of PDN-gate has mentioned in Appendix: B.

4.3 LTE CORE NETWORK FOR L2-TUNNEL

Follow same procedure as GRE configuration in LTE core network. Create separate APN template, subtemplate and QoS template in HSS. New DNS naptor record create in side MME to resolve LTE node address that use for L2TP tunnel setup. Create APN, routing instance and IP address pool in PDN-gateway for L2TP tunnel setup. Connect L2TP server to the PDN-gateway and assign the connected port to the routing-instance create for the L2TP tunnel. Direct IP packets from L2TP client to the L2TP server, creating default route to L2TP server in the routing-instance. Appendix: C has LTE core network configuration for L2TP tunnel.

L2TP server connected to the PDN gateway need to have telnet, SSH and PPP service available to connect with L2TP client. L2TP server and client connect through the virtual interface created in both devices using PPP (point-to-point protocol) and use CHAP authentication which is protect tunnel against Replay attacks. Create L2TP group binding virtual template interface, and create tunnel name and password that should be identical in both server and client. Server side configuration of the L2TP server as in Appendix: D.

4.4 LTE ACCESS NETWORK FOR GRE

Main entity of LTE access network is eNodeB and LTE-wireless access route. eNodeB does not need any modification to have GRE and IPSec tunnels. One end of GRE tunnel create inside LTE-wireless access router and all IP packets inside the LTE-wireless access router direct to the tunnel using static route inside the router.

```
# ip route
192.168.20.62 dev gre3  scope link
119.235.0.4 via 10.32.1.1 dev eth1.1
10.50.3.54 via 10.32.1.1 dev eth1.1
```

```
8.8.8.8 via 10.32.1.1 dev eth1.1
10.32.1.0/26 dev eth1.1  proto kernel  scope link  src 10.32.1.32
192.168.3.0/24 dev br0  proto kernel  scope link  src 192.168.3.1
10.10.10.0/24 via 192.168.3.2 dev br0
169.254.0.0/16 dev eth1  proto kernel  scope link  src 169.254.9.221
default via 10.32.1.1 dev eth1.1
#
```

Detailed configuration in the LTE-wireless access router have attached to the Appendix: B.

4.5 LTE ACCESS NETWORK FOR L2TP

eNodeBs in LTE access network don't need to configure for creating L2TP tunnels that make fast deployment and low maintenance for layer-2 tunnels over LTE network. Configuration of the client is identical with L2TP sever except default route which forward all IP packets to LTE wireless router.

4.6 MPLS NETWORK FOR GRE

Virtual routing and forwarding (VRF) that is a technology use in routers to keep multiple instances of routing tables to function simultaneously, create in the MPLS edge router for each and every GRE (L3) tunnel. VRF make flexibility to extend the tunnels through other wireless technologies like WiMAX.

Sub-interface that belong to the VRF in the route mark the IP packet with IEEE dot1q tag and forward to the PDN gateway. Virtual interface (interface tunnel) create in MPLS edge router function as one end of the GRE tunnel, take all IP packets coming to the VRF and create the GRE tunnel with LTE wireless router. Configuration of MPLS network has in Appendix

4.7 MPLS NETWORK FOR L2TP

Extending L2TP tunnel where location does not have LTE network coverage only require the configuration in MPLS network. IP data packet mark with IEEE dot1q tag in L2TP server forward to the MPLS edge router sub interface and create x-connect (is a technology to deliver L2 traffic over L3 network) with other MPLS edge route where tunnel should extend. Router configuration as follows for the L2TP tunnel extend through MPLS network.

```
set protocols l2circuit neighbor 10.12.0.8 interface ge-1/1/1.599 virtual-circuit-id 599
set protocols l2circuit neighbor 10.12.0.8 interface ge-1/1/1.599 description "*** L2_TUNNEL_EXTEND ***"

set interfaces ge-1/1/1 unit 599
set description "*** L2_TUNNEL_EXTEND ***";
set encapsulation vlan-ccc;
set vlan-id 599;
```

4.8 IPSEC TUNNEL IMPLIMENTATION

IPSec tunnel create through the L2-tunnels or GRE tunnels do not need to do any further configuration on LTE core network devices. But route at IPSec tunnel end points need to programme for IPSec tunnels. Create admin user account in the router with highest privileges.

```
aaa
 authentication-scheme default
```

```
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password irreversible-cipher %^%#KfnT"#w*v&5%~3#~Kmi>/5I<
 local-user admin privilege level 15
 local-user admin service-type terminal http
```

Define the IKE related information in the router that are authentication algorithm, encryption algorithm, Pre-shared key and IKE remote peer IP address. IKE related information need to be match in both devices to create IPSec tunnel.

```
ike proposal 22
 encryption-algorithm aes-cbc-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer jjj v2
 pre-shared-key simple test
 ike-proposal 22
 local-address 192.168.3.2
 remote-address 192.168.3.1
```

Define IPSec related information as IKE-phase 2 that are IPSec security protocol, authentication algorithm use by AH, authentication algorithm use by ESP and access list for mark the data that needs encrypt using IPSec and IPSec policy to interface for encrypt the date that going through the interface.

```
acl number 3001
 rule 22 permit icmp
ipsec policy kkk-policy 22 isakmp
 security acl 3001
 pfs dh-group5
 ike-peer jjj
 proposal kkk-prop
#
ipsec proposal kkk-prop
 transform ah
 ah authentication-algorithm md5
interface GigabitEthernet0/0/5
 undo portswitch
 ip address 192.168.3.2 255.255.255.0
 ipsec policy kkk-policy
```

4.9 SOFTWARE FOR ROUTER CONFIGURATION

Programme the routers for L2/L3 tunnel and IPSec tunnel need expert’s knowledge and skills. Routers implement at the tunnel end points are beyond the reachability of engineers through internet. The small software has developed using java programme to simplify the configuration of the LTE wireless router.

User logging to the LTE wireless router through the software use SSH connection. The software request the required details for create L2 (GRE) tunnel, configure LAN IP range and create static route. Below java code shows the software requested details for configuring the tunnel. Appendix G has the complete java code written for the software.

```
Scanner input = new Scanner(System.in);
        /*System.out.println("-----------LOGIN DETAILS -----------------");
        System.out.print("Enter Host IP: ");
        hostip = input.nextLine();
        System.out.print("Enter username: ");
        usern = input.nextLine();
        System.out.print("Enter password: ");
        pass = input.nextLine();*/
        System.out.println("--------------- GRE VPN ------------------");
        System.out.print("Enter GRE server IP : ");
        server = input.nextLine();
        System.out.print("Enter GRE local  IP : ");
        local = input.nextLine();
        System.out.print("Enter GRE remote IP : ");
        remote = input.nextLine();
        System.out.println("------------- Static Route -----------------");
        System.out.print("Enter destination IP :");
        dest=input.nextLine();
        System.out.print("Enter mask :");
        mask=input.nextLine();
        System.out.println("------------- LAN IP Setup ------------------");
        System.out.print("Enter IP address :");
        ip=input.nextLine();
        System.out.print("Enter subnet mask :");
        subnet=input.nextLine();
        System.out.print("Enter broadcast IP :");
        broad=input.nextLine();
```

CHAPTER 5: RESULTS AND ANALYSIS

5.1 LAYER-3 TUNNEL

L3-tunnel create connecting two end devices for packet capturing at PDN-gateway. L3-tunnel starting at LTE wireless router and extend to the eNodeB then S-GW, PDN-gateway and MPLS edge router. MPLS edge router has virtual routing table for end devices connecting through L3-tunnels. There are three possible locations to capture L3-tunnel traffic that are starting point, end point and PDN-gateway. L3-tunnel start point and end point are virtually build interfaces inside the route and connecting to other end of tunnel through LTE wireless interface. PDN-gateway is in the place between L3-tunnel end points and it is outside the user's premises. Specify the IMSI belongs to L3-tunnel user at PDN-gateway and capture the data relevant to that IMSI. The below figure shows that the captured tunnel traffic at PDN-gateway without IPSec tunnel inside L3-tunnel.

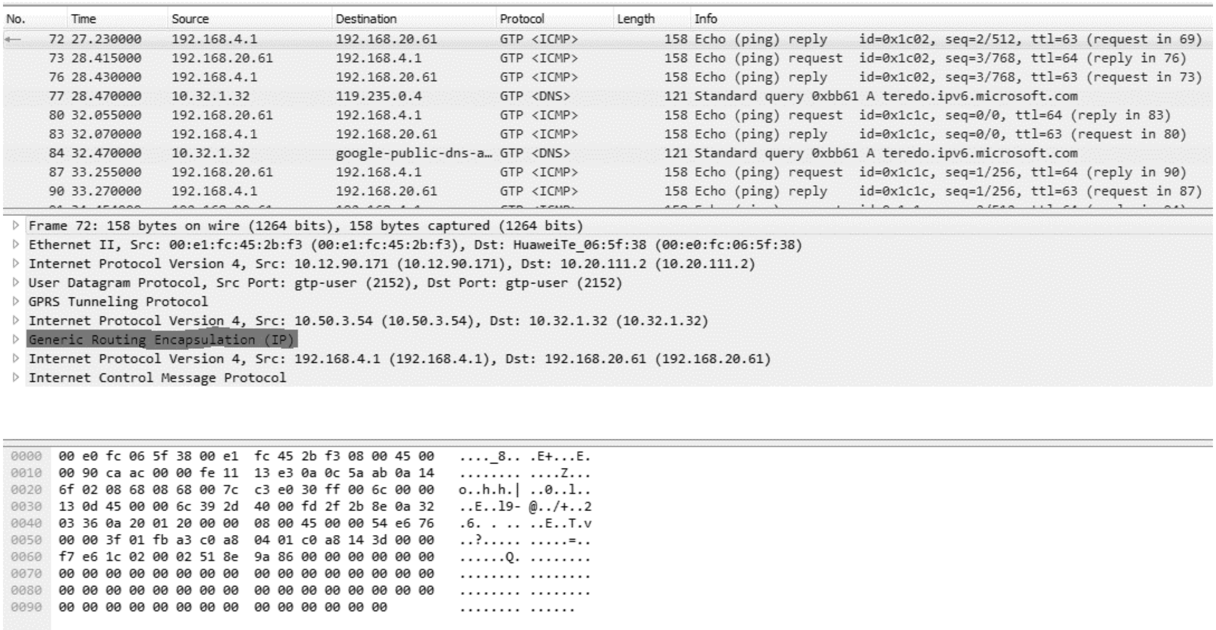

Figure 20 : Packet capture of L3-tunnel at PDN-gateway

The above figure shows the packet capture of GTP protocol which is use in LTE networks for carrying data traffic. It show the data frame at physical layer (Layer-1), Ethernet packet at data link layer (Layer-2), IP packet at network layer (Layer-3), User Datagram Protocol (UDP) at transport layer. GTP and GRE tunnels inside the transport layer. GTP tunnel is default LTE tunnel for user's data traffic, and GRE tunnel (L3-tunnel) which connect two end devices through LTE network.

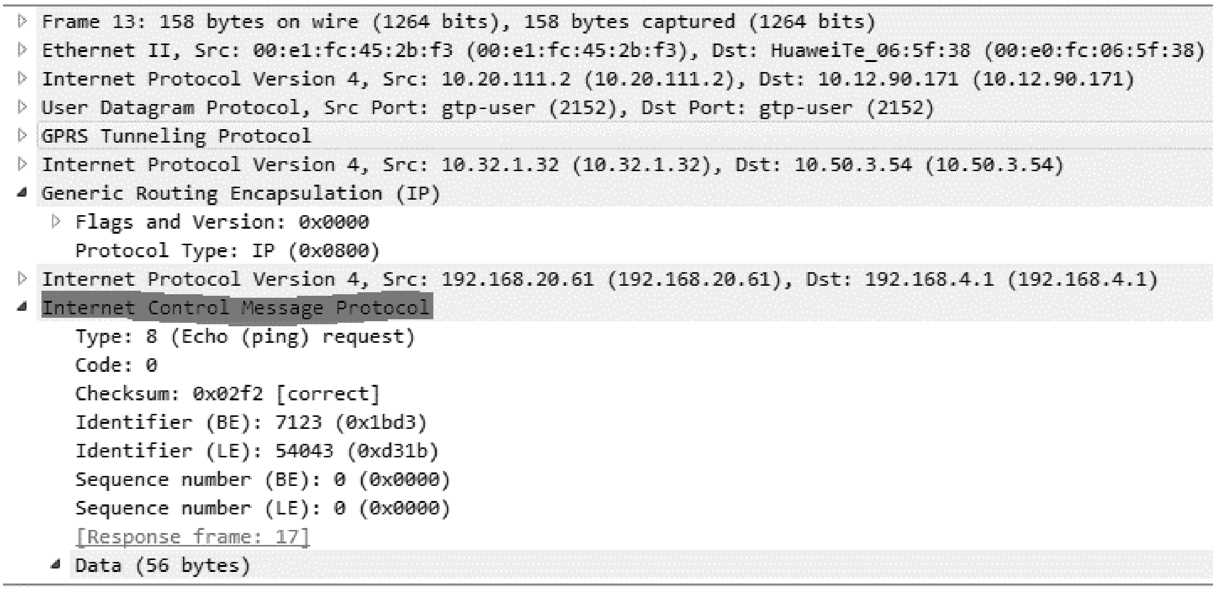

Figure 21 : Unencrypted data inside L2-tunnel packet capture at PDN-gateway

This packet capture has taken when two end devices PING to each other through L3-tunnel. The above figure shows the data inside GRE tunnel which is ICMP packet use for PING request and not encrypted. Data going through L3-tunnel is visible to everyone who can capture the data in wireless transmission media (LTE wireless router to eNodeB) or in the ISP core network.

5.2 IPSEC TUNNEL INSIDE L3-TUNNEL

The router connect with the LTE wireless router has configured for the creation of IPSec tunnels and use access list rule to take the traffic into IPSec tunnel. The below figure shows the captured traffic at LTE wireless router. IPSec L3-tunnel starting at the router that connected to the LTE wireless router and IPSec tunnel going through the LTE wireless router. Capturing data at LTE wireless router have L3-tunneling information and IPSec tunnelling except LTE-GTP tunnelling information.

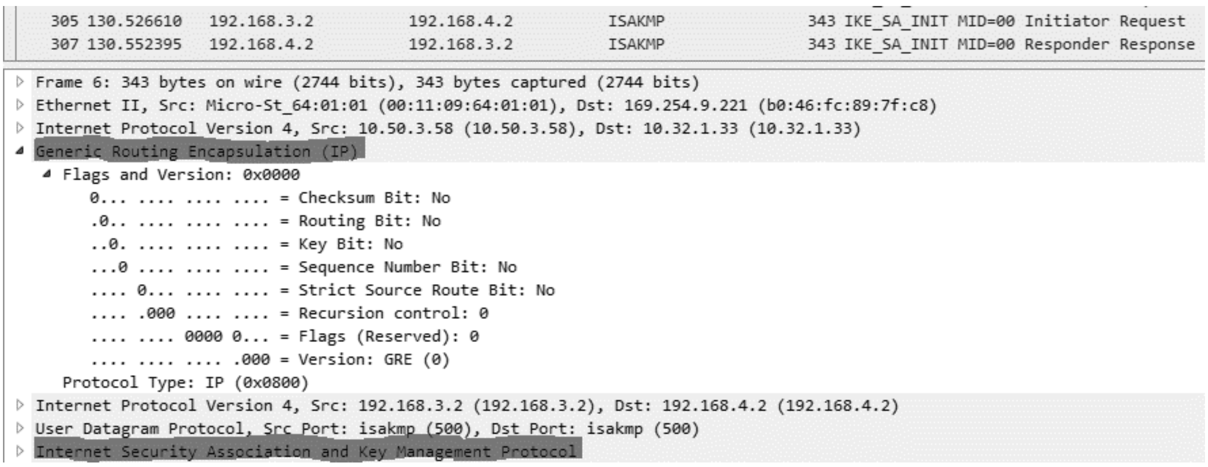

Figure 22 : IPSec tunnel Packet capture at LTE wireless router

The above figure shows the L3-tunneling information and inside the L3-tunnel, ISAKMP data which is protocol suit use for exchanging the IPSec related key information. L3-tunnel make the communication link between two end devices to establish IPSec tunnel. The below figure shows the encrypted payload inside ISAKMP. The IPSec tunnel inside L2-tunnel (GRE) make more secure link between end-devices through ISP network without using any public IP address. Appendix H contain the details of created IPSec tunnel taken from the end-routes to verify the IPSec tunnel information.

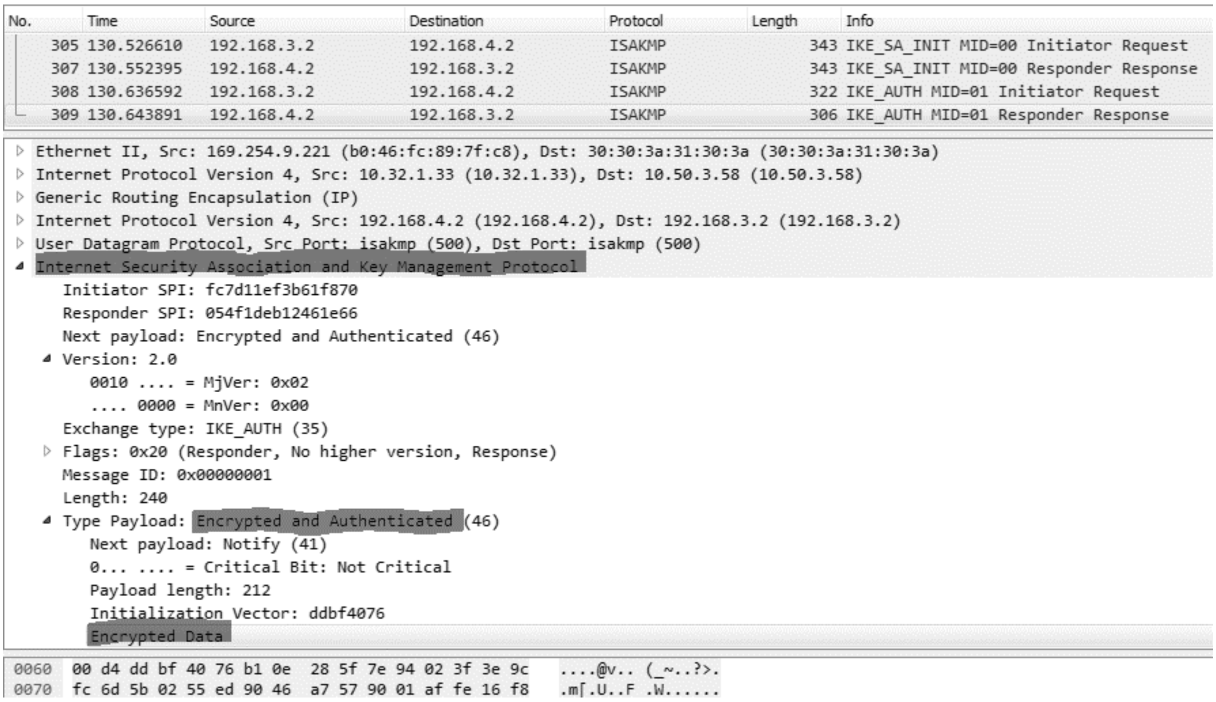

Figure 23 : Encrypted data inside IPSec tunnel, packet capture at LTE wireless router

5.3 LAYER-2 TUNNEL

The below figure show the packet capture that has taken at PDN-gateway without IPSec tunnel inside L2-tunnel. L2TP header wrapped the whole data packet and send to the other end of L2-tunnel through the LTE network. LTE network tunnelling protocol (GTP), wrap the whole data packet inside it. Below figure show the tunnel wrapping of the data packets that transmitting through the LTE network. Data inside that packet is readable to anyone who can capture the data. The below figure shows the ICMP packets and its payload inside the GTP packets are readable to anyone.

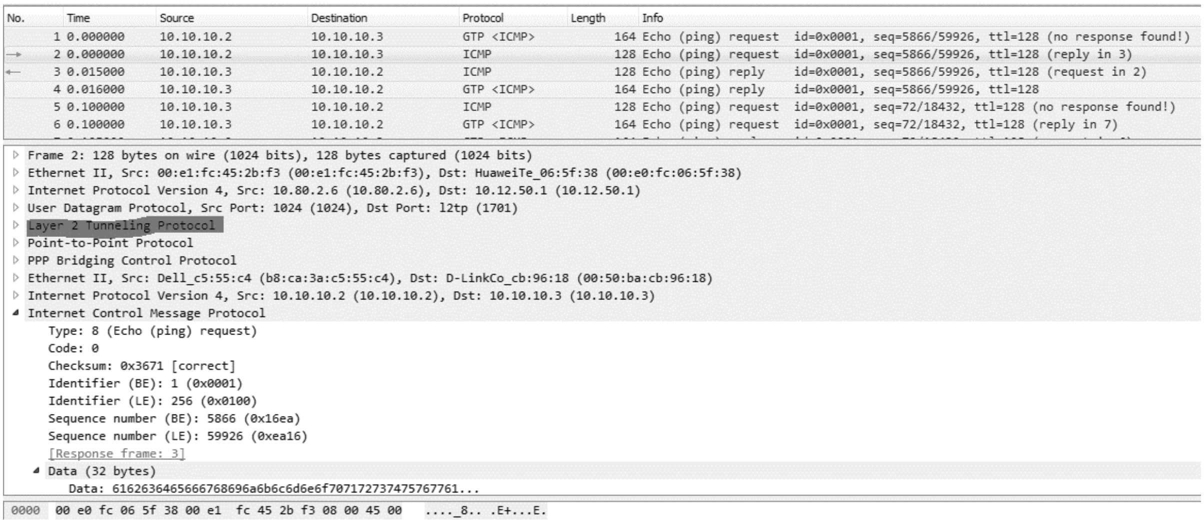

Figure 24 : L2-tunnel captured data without IPSec

5.4 IPSEC TUNNEL INSIDE L2-TUNNEL

IPSec secured tunnel has create inside L2-tunnel and captured the data at PDN-gateway that is middle point of the secured tunnel. The below figure show the encrypted data inside the L2-tunnel with IPSec configured encryption. The encrypted payload of the data packet is not readable. Appendix I contain the IPSEC tunnel information taken at tunnel end point routers that specify the number of data packets transmit through the tunnel and key establishment.

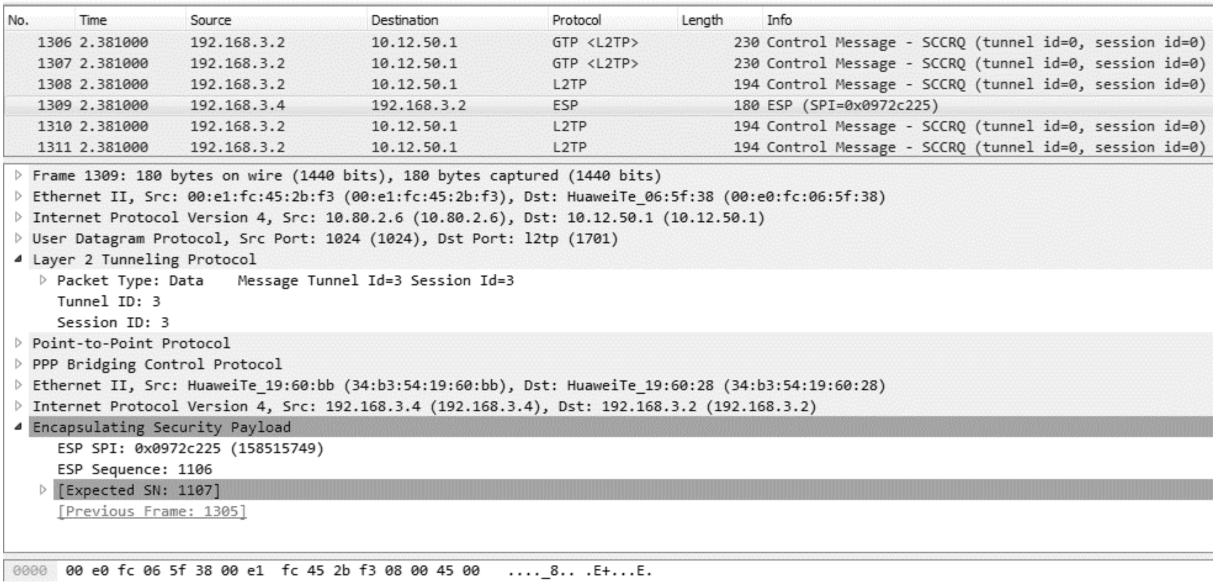

Figure 25 : L2-tunnel captured data with IPSec

CHAPTER 6: CONCLUSION AND FUTURE WORK

6.1 CONCLUSION

The thesis has organized by first introducing about the topic and then discussing literature and related works, design of solution, implementation, results-analysis and conclusion. Data passing through LTE core network are not secure enough and person who can capture the data can read information in it. Captured data at PDN-gateway without any tunnel in use, shows the information inside the data packets. All security mechanisms in LTE have implemented for protecting data in LTE access network. Anyone can capture the date at backend of LTE core network can read the information inside that data packets.

Layer-3 tunnel created using GRE protocol does not have any protection over information it's transmitting. Packet capture at the PDN-gateway of the L3-GRE tunnel shows that there is no any protection for the data inside the captured packets. L3-GRE tunnel with IPSec protocol suit encrypt the data in LTE network can use as VPN solution for enterprise network. Packet capture of L3-GRE tunnel with IPSec encrypted at PDN-gateway shows that its payload has encrypted and no one can read the information over it.

Layer-2 tunnel in LTE network create Virtual Private LAN Network (VPLS) like connectivity which is equal to mobile VPLS network. Information inside the data packets that passing through L2-tunnel is not secured. Packet captured at PDN gateway shows that information inside the packet payload. IPSec encrypted tunnel inside L2-tunnel create secured data payload that can only decrypt at the other end of the tunnel. But over heads data in the IP packets are very high with IPsec-GRE and L2TP-IPSec. Packet capture of L2TP-IPSec encrypted tunnel at the PDN gateway shows that L2TP tunnel packet payload has encrypted.

6.2 FUTURE WORKS

The device at user's side that use for creating Layer-3 tunnel has two module which are out-door antenna and indoor-router. Using router with high gain antenna reduce the devices at user's side make simple system with easier mobility. Reducing the number of devices at tunnel end points to make simple system that lower the maintenance cost. Reducing number of devices at LTE front end network is possible by making LTE back end more secure. Providing voice call facility with VPN system is another interesting feature for the users of VPN system that make complete solution for enterprises communication needs. Other than simple Layer-2 point-point and point-to-multipoint VPN connectivity, it will required to send IEEE.1q marked packets through the Layer-2 tunnels. The tunnel response for that type of data traffic need to be analysed. There is a small packet drop in the Layer-2 point-to-multipoint tunnelling system that need to be address. Monitoring system is very important for trouble shooting the tunnelling system. Develop the monitoring system to monitor real time traffic through the Layer-2 and Layer-3 tunnels make easier and fast the trouble shooting process. Develop the software for configure L2 and L3 tunnels at tunnel end points that make the tunnel creation process easier for low skilled people.

REFERENCES

[1] C. Cox, AN INTRODUCTION TO LTE, John Wiley & Sons Ltd, 2012.

[2] Alcatel-Lucent, “www.cse.unt.edu,” [Online]. Available: http://www.cse.unt.edu/~rdantu/FALL_2013_WIRELESS_NETWORKS/LTE_Alcatel_White_Paper.pdf. [Accessed 02 Dec 2016].

[3] S. Ahmadi, LTE-Advanced: A Practical Systems Approach to Understanding 3GPP LTE Releases 10 and 11 Radio Access Technologies, UK: Acadamic press, 2013.

[4] B. SEBIRE, “Specification #: 36.300,” 06 Aprial 2007. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2430. [Accessed 20 Nov 2016].

[5] N. S. Anastasios Bikos, “LTE/SAE security issues on 4G wireless networks,” Researchgate, 04 June 2015. [Online]. Available: https://www.researchgate.net/publication/236117981_LTESAE_security_issues_on_4G_wireless_networks. [Accessed 10 Jan 2017].

[6] D. Forsberg, LTE Security, United state: John Wiley, 2010.

[7] B. Chinni, “MMBI White Paper on Use of MPLS in LTE,” Feb 2010. [Online]. Available: https://www.broadband-forum.org/marketing/download/mktgdocs/MR-238.pdf. [Accessed Nov 2016].

[8] D. T. a. B. Vachon, Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide, united state: cisco publisher, 15 Jan 2015, pp. 34-36.

[9] academlib.com, “http://academlib.com,” academlib.com, 2014. [Online]. Available: http://academlib.com/26733/computer_science/layer_tunneling_protocol_l2tpv3. [Accessed 24 Nov 2016].

[10] S. Malik, Network Security Principles and Practices, united state: cisco publisher, Nov 15 2002.

[11] J. Technologies, Network Protocols Handbook, California: Javvin technologies, 2005.

[12] networks, Juniper, “GPRS Tunneling Protocol (GTP) Overview,” Juniper Networks, 14 Feb 2013. [Online]. Available: http://www.juniper.net/techpubs/en_US/junos-mobility12.1/topics/concept/gtp-mobility-protocols-overview.html. [Accessed 2016 Dec 19].

[13] B. P. a. Y. Saifullah, IP in Wireless Networks, New Jersey: IP in Wireless Networks, 2003.

[14] M. H. Sherif, Protocols for Secure Electronic Commerce, Second Edition (Advanced & Emerging Communications Technologies), Florida: CRC Press, 2003.

[15] M. Silander, "The ISAKMP framework," Department of Computer Science Helsinki University of Technology, 24 Aprial 1999. [Online]. Available: http://www.tml.tkk.fi/Opinnot/Tik-110.551/1999/papers/02SecurityInIP/isakmp.html. [Accessed 15 Jan 2017].

[16] A. G. Madhusanka Liyanage, "Secured VPN Models for LTE Backhaul Networks," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*, 2012.

[17] F. Z. L. K. Salima Smaoui, "IPSec tunnel establishment for 3GPP-WLAN interworking," in *Informatics and Systems (INFOS), 2012 8th International Conference*, 2012.

[18] A. H. M. W. Ahmed Laguidi, "Secure HeNB network management based VPN IPSec," in *Next Generation Networks and Services (NGNS)*, 2012.

Appendix A: HSS CONFIGURATION

```
PGW    #099031
%%LST OPTGPRS: IMSI="413040116000872";%%
RETCODE = 0 SUCCESS0001:Operation is successful

                          IMSI = 413040000000000
                          ISDN = 94119000000
                 CHARGE_GLOBAL = NONE
                        CNTXID = 1
                      APN_TYPE = EPS_APN
                      APNTPLID = 605
                DEFAULTCFGFLAG = TRUE
               WILDCARDAPNFLAG = FALSE
                  EPS_QOSTPLID = 605
                       PDPTYPE = IPV4
                        ADDIND = STATIC
                        PDPADD = 10.32.1.32
                         VPLMN = FALSE
                        CHARGE = NORMAL

Total count = 14

There is together 1 report

---    END

PGW    #099039
%%LST EPSQOSTPL: HLRSN=1, TPLID=605;%%
RETCODE = 0 SUCCESS0001:Operation is successful

                         TPLID = 605
                       TPLNAME = 4gvpn
                    QOSCLASUID = 6
                      PRILEVEL = 1
                AMBRMAXREQBWUL = 104857600
                AMBRMAXREQBWDL = 104857600

Total count = 6
There is together 1 report

---    END

PGW    #099079
%%LST OPTGPRSTPL: HLRSN=1, TPLID=605;%%
RETCODE = 0 SUCCESS0001:Operation is successful

                         HLRSN = 1
                         TPLID = 605
                       TPLNAME = 4gvpn
                        CNTXID = 1
                      APN_TYPE = EPS_APN
                      APNTPLID = 605
                DEFAULTCFGFLAG = TRUE
                  WILDCARDFLAG = FALSE
                  EPS_QOSTPLID = 605
                         VPLMN = FALSE
                       PDPTYPE = IPV4
                        CHARGE = NORMAL


Total count = 12
```

```
There is together 1 report

---    END

PGW    #099087
%%LST SUBTPL: HLRSN=1, TPLID=605;%%
RETCODE = 0 SUCCESS0001:Operation is successful

                         HLRSN = 1
                         TPLID = 605
                       TPLNAME = 4gvpn
                      CARDTYPE = USIM
                           NAM = BOTH
                      CATEGORY = COMMON
                  USERCATEGORY = NORMAL

"Basic Service"
                    Emergency Call (TS12)
                   DEFAULTCALL = Telephony (TS11)

"GPRS Data"
                  OPTGPRSTPLID = 605
                 CHARGE_GLOBAL = NONE

                          SMDP = Deliver From MSC
                      NAEA_CIC = NOTPROV
                        NLRInd = NONE
                          VVDN = NOTPROV
                           ARD = NOTPROV
               WLANNOTALLOWED = FALSE
        CDMA2000_1XNOTALLOWED = FALSE
               HRPDNOTALLOWED = FALSE
                UMBNOTALLOWED = FALSE
              EHRPDNOTALLOWED = FALSE
                          CARP = NOTPROV
                      RROption = ALL_PLMNS
                         EMLPP = NOTPROV
                     EMLPP_COU = SUBSCRIBER
                           VBS = NOTPROV
                          VGCS = NOTPROV
                     ECATEGORY = NOTPROV
                           IST = NOTPROV
                           DIC = NOTPROV
                 ROUTECATEGORY = NOTPROV
                  CALLREDIRECT = NOTPROV
                         MERBT = NOTPROV
             EXEXROUTECATEGORY = NOTPROV
                       NIRPROV = FALSE
                         RZONE = 0
                          CCBS = NOTPROV
                    CCBSTARGET = PROV
                     SMSINPROV = FALSE
                          SKEY = 0
                          TAMM = FALSE
                           CPP = NOTPROV
                          ELCS = NOTPROV
"EPS Data"
                     AMBRMAXUL = 100000000
                     AMBRMAXDL = 100000000
                   NON3GPPSUPP = FALSE

"M2M"
```

```
                    IMEILCKPROV = FALSE
                      M2MNOTIFY = NOTPROV

Total count = 136

There is together 1 report

---    END
```

Appendix B: CONFIGURATION OF PDN-GATEWAY

```
<UGW>display ip pool 4gvpn
Pool Information
----------------
             Pool Name  =  4gvpn
             Pool Type  =  Local
             Pool Lock  =  Unlock
     Pool Alarm Report  =  Disable
  single-ip-allocation  =  Disable
          Pool IP Type  =  IPv4
          VPN Instance  =  4gvpn
    IP Release Time(s)  =  0
         Pool IP Lease  =  Disable
Wait Release IP Number  =  0
         Section Count  =  2
     Conflict IP Count  =  0
       IP Total Number  =  0
        IP Used Number  =  0
     IP Invalid Number  =  0
              IP Usage  =  0

           Conflict IP  =  NULL

        Section Number  =  0
          Section Type  =  Static
          Section Lock  =  Unlock
      Section Start IP  =  ###.###.###.###
        Section End IP  =  ###.###.###.###

        Section Number  =  1
          Section Type  =  Static
          Section Lock  =  Unlock
      Section Start IP  =  ###.###.###.###
        Section End IP  =  ###.###.###.###

         Bind APN Name  =  4gvpn


#
apn 4gvpn
 vpn-instance 4gvpn
 content-awareness disable
 service-report switch global
 access-mode transparent-non-authentication
 framed-route-mode disable
 address-allocate ipv4 local radius-prior disable ipv6 local radius-prior
disable
 address-support ipv4 enable ipv6 enable preference ipv4
 address-allocate-preference enable
 ppp-access authentication disable
 ppp-access address-allocate local radius-prior disable
 virtual-apn disable
 address-inherit enable
 apn-restriction disable
 remove-domain-name radius disable
 remove-domain-name lns disable
 roaming-user-access sgw enable visiting-user-access enable
 roaming-user-access ggsn-pgw enable visiting-user-access enable
 session-timeout disable
 idle-timeout disable
 static-ip hlr-hss-provided enable conflict ignore route enable all
 select-mode-check disable
```

```
 lock disable
 dns ipv4 primary-ip #.#.#.# secondary-ip #.#.#.#
 address-pool 4gvpn
 volume-statistic-mode layer-all
 aaa-apn-secondauth disable
 apn-type-select perf service cg service aaaacct service aaaauth service ocs
service pcrf service header-enrichment service
 plmn serving-node-mapping enable
 rat sgsn-sgw-mapping enable
 multiple-service-mode radius
 radius-disconnect enable
 offline-charge-binding ggsn #######_cdr_template pgw ########_cdr_template
sgw #######_cdr_template
 radius acctctrl accounting-update enable
 pcc-switch enable
 pcc-default reporting-level rg metering-method volume
 user-profile-group-binding data_only_test
#
```

Appendix C: L2TP CORE NETWORK CONFIGURATION

```
apn l2vpn
 vpn-instance l2vpn
 content-awareness disable
 service-report switch global
 access-mode transparent-non-authentication
 framed-route-mode disable
 address-allocate ipv4 local radius-prior disable ipv6 local radius-prior
disable
 address-support ipv4 enable ipv6 enable preference ipv4
 address-allocate-preference enable
 ppp-access authentication disable
 ppp-access address-allocate local radius-prior disable
 virtual-apn disable
 address-inherit enable
 apn-restriction disable
 remove-domain-name radius disable
 remove-domain-name lns disable
 roaming-user-access sgw enable visiting-user-access enable
 roaming-user-access ggsn-pgw enable visiting-user-access enable
 session-timeout disable
 idle-timeout disable
 static-ip hlr-hss-provided enable conflict ignore route enable all
 select-mode-check disable
 lock disable
 address-pool l2vpn
 volume-statistic-mode layer-all
 aaa-apn-secondauth disable
 apn-type-select perf service cg service aaaacct service aaaauth service ocs
service pcrf service header-enrichment service
 plmn serving-node-mapping enable
 rat sgsn-sgw-mapping enable
 multiple-service-mode radius
 radius-disconnect enable
 offline-charge-binding ggsn lankabellte_cdr_template pgw
lankabellte_cdr_template sgw lankabellte_cdr_template
 radius acctctrl accounting-update enable
 pcc-switch enable
 pcc-default reporting-level rg metering-method volume
 user-profile-group-binding data_only_test
 acl-binding direction up-in acl acl_f_lns
 tcp-mss 1400

ip pool l2vpn local ipv4
  vpn-instance l2vpn
  section 0 10.10.2.1 10.10.2.254 static
  alarm-report disable

ip vpn-instance l2vpn
 description l2vpn_common
 ipv4-family
  route-distinguisher 2002:1
```

Appendix D: L2TP SEVER CONFIGURATION

```
local-user test1 password cipher %@%@Z=/#,QLD&O4+Z$9"x_[H,L9T%@%@
 local-user test1 privilege level 15
 local-user test1 service-type telnet ssh ppp

interface Eth-Trunk1.2002
 description *** L2VPN_connect_to_PDN-gateway ***
 dot1q termination vid 2002
 ip address 10.2.12.1 255.255.255.252

interface Virtual-Template1
 bridge 1
 ppp authentication-mode chap
 ppp chap password cipher %@%@~w7uBs]q9OU_fJB4`*$Q#N*A%@%@

l2tp-group 1
 allow l2tp virtual-template 1 remote lac1
 tunnel password cipher %@%@ns"]UwnH@>n+5AN-_:,N,&h~%@%@
 tunnel name lns
```

Appendix E: MPLS CONFIGURATION FOR GRE

```
ip vrf test-link
 rd 65001:1153512000
 route-target export 65001:1153512000
!
!
ip route vrf test-link 10.10.10.0 255.255.255.0 192.168.3.1
ip route vrf test-link 10.32.1.32 255.255.255.255 10.50.3.53
ip route vrf test-link 10.32.1.33 255.255.255.255 10.50.3.57
ip route vrf test-link 10.32.1.34 255.255.255.255 10.50.3.61
ip route vrf test-link 10.32.1.35 255.255.255.255 10.50.3.65
ip route vrf test-link 192.168.3.0 255.255.255.0 192.168.20.61
ip route vrf test-link 192.168.4.0 255.255.255.0 192.168.20.65
ip route vrf test-link 192.168.5.0 255.255.255.0 192.168.20.69
ip route vrf test-link 192.168.6.0 255.255.255.0 192.168.20.73
!
interface Tunnel3514
 description *** Group-3 ***
 ip vrf forwarding test-link
 ip address 192.168.20.62 255.255.255.252
 tunnel source 10.50.3.54
 tunnel destination 10.32.1.32
 tunnel vrf test-link

interface GigabitEthernet2/4.3514
 description *** GRE_Tunnel ***
 encapsulation dot1Q 3514
 ip vrf forwarding test-link
 ip address 10.50.3.54 255.255.255.252
end
```

Appendix F: GRE TUNNEL CONFIGURATION

```
#ip tunnel add gre3 mode gre remote 10.50.3.54 local any ttl 255
#ip link set gre3 up
#ip addr add 192.168.20.61 dev gre3
#ip route add 192.168.20.62 dev gre3
#ip route del 0.0.0.0/0
#ip route add 0.0.0.0/0 via 10.32.1.1
#ip route add 10.50.3.54/255.255.255.255 dev eth1.1 proto static
#ifconfig br0 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255

# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.20.62   0.0.0.0         255.255.255.255 UH    0      0        0 gre3
119.235.0.4     10.32.1.1       255.255.255.255 UGH   0      0        0 eth1.1
10.50.3.54      10.32.1.1       255.255.255.255 UGH   0      0        0 eth1.1
8.8.8.8         10.32.1.1       255.255.255.255 UGH   0      0        0 eth1.1
10.32.1.0       0.0.0.0         255.255.255.192 U     0      0        0 eth1.1
192.168.3.0     0.0.0.0         255.255.255.0   U     0      0        0 br0
10.10.10.0      192.168.3.2     255.255.255.0   UG    0      0        0 br0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth1
0.0.0.0         10.32.1.1       0.0.0.0         UG    0      0        0 eth1.1
#

# ifconfig
br0       Link encap:Ethernet  HWaddr E0:41:36:8E:D0:C7
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::542f:30ff:fe56:f188/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9018 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8280 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1055397 (1.0 MiB)  TX bytes:4739705 (4.5 MiB)

eth0      Link encap:Ethernet  HWaddr E0:41:36:8E:D0:C7
          inet6 addr: fe80::e241:36ff:fe8e:d0c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9055 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8281 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1087985 (1.0 MiB)  TX bytes:4754249 (4.5 MiB)

eth1      Link encap:Ethernet  HWaddr E0:41:36:8E:D0:C0
          inet addr:169.254.9.221  Bcast:169.254.255.255  Mask:255.255.0.0
          inet6 addr: fe80::e241:36ff:fe8e:d0c0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6101 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:332327 (324.5 KiB)  TX bytes:464578 (453.6 KiB)

eth1.1    Link encap:Ethernet  HWaddr E0:41:36:8E:D0:C0
          inet addr:10.32.1.32  Bcast:10.32.1.63  Mask:255.255.255.192
          inet6 addr: fe80::e241:36ff:fe8e:d0c0/64 Scope:Link
          UP BROADCAST RUNNING NOARP ALLMULTI MULTICAST  MTU:1400  Metric:1
          RX packets:42 errors:0 dropped:0 overruns:0 frame:0
          TX packets:933 errors:0 dropped:0 overruns:0 carrier:0
```

```
          collisions:0 txqueuelen:0
          RX bytes:4534 (4.4 KiB)  TX bytes:88563 (86.4 KiB)

gre3      Link encap:UNSPEC  HWaddr 0A-20-01-20-00-00-00-00-00-00-00-00-
00-00-00
          inet addr:192.168.20.61  P-t-P:192.168.20.61
Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP  MTU:1376  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:40 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1064 (1.0 KiB)  TX bytes:3164 (3.0 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:305 errors:0 dropped:0 overruns:0 frame:0
          TX packets:305 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17775 (17.3 KiB)  TX bytes:17775 (17.3 KiB)
```

Appendix G: JAVA CODE OF THE SOFTWARE

```
package sshclient;

import org.apache.oro.text.regex.MalformedPatternException;

import com.jcraft.jsch.ChannelShell;
import com.jcraft.jsch.JSch;
import com.jcraft.jsch.Session;

import expect4j.Closure;
import expect4j.Expect4j;
import expect4j.ExpectState;
import expect4j.matches.Match;
import expect4j.matches.RegExpMatch;
import java.util.ArrayList;
import java.util.Hashtable;
import java.util.List;
import java.util.Scanner;

public class SSHClient {

    private static final int COMMAND_EXECUTION_SUCCESS_OPCODE = -2;
    private static String ENTER_CHARACTER = "\r";
    private static final int SSH_PORT = 22;
    private List<String> lstCmds = new ArrayList<String>();
    private static String[] linuxPromptRegEx = new String[]{"\\>","#", "~#"};

    private Expect4j expect = null;
    private StringBuilder buffer = new StringBuilder();
    private String userName;
    private String password;
    private String host;

    /**
     *
     * @param host
     * @param userName
     * @param password
     */
    public SSHClient(String host, String userName, String password) {
        this.host = host;
        this.userName = userName;
        this.password = password;
    }
    /**
     *
     * @param cmdsToExecute
     */
    public String execute(List<String> cmdsToExecute) {
        this.lstCmds = cmdsToExecute;

        Closure closure = new Closure() {
            public void run(ExpectState expectState) throws Exception {
                buffer.append(expectState.getBuffer());
            }
        };
        List<Match> lstPattern =  new ArrayList<Match>();
        for (String regexElement : linuxPromptRegEx) {
            try {
                Match mat = new RegExpMatch(regexElement, closure);
                lstPattern.add(mat);
            } catch (MalformedPatternException e) {
```

```
                e.printStackTrace();
            } catch(Exception e) {
                e.printStackTrace();
            }
        }

        try {
            expect = SSH();
            boolean isSuccess = true;
            for(String strCmd : lstCmds) {
                isSuccess = isSuccess(lstPattern,strCmd);
                if (!isSuccess) {
                    isSuccess = isSuccess(lstPattern,strCmd);
                }
            }

            checkResult(expect.expect(lstPattern));
        } catch (Exception ex) {
            ex.printStackTrace();
        } finally {
            closeConnection();
        }
        return buffer.toString();
    }
    /**
     *
     * @param objPattern
     * @param strCommandPattern
     * @return
     */
    private      boolean      isSuccess(List<Match>      objPattern,String
strCommandPattern) {
        try {
            boolean isFailed = checkResult(expect.expect(objPattern));

            if (!isFailed) {
                expect.send(strCommandPattern);
                expect.send(ENTER_CHARACTER);
                return true;
            }
            return false;
        } catch (MalformedPatternException ex) {
            ex.printStackTrace();
            return false;
        } catch (Exception ex) {
            ex.printStackTrace();
            return false;
        }
    }
    /**
     *
     * @param hostname
     * @param username
     * @param password
     * @param port
     * @return
     * @throws Exception
     */
    private Expect4j SSH() throws Exception {
        JSch jsch = new JSch();
        Session session = jsch.getSession(userName, host, SSH_PORT);
        if (password != null) {
```

```
            session.setPassword(password);
        }
        Hashtable<String,String> config = new Hashtable<String,String>();
        config.put("StrictHostKeyChecking", "no");
        session.setConfig(config);
        session.connect(60000);
        ChannelShell channel = (ChannelShell) session.openChannel("shell");
        Expect4j    expect    =    new    Expect4j(channel.getInputStream(),
channel.getOutputStream());
        channel.connect();
        return expect;
    }
    /**
     *
     * @param intRetVal
     * @return
     */
    private boolean checkResult(int intRetVal) {
        if (intRetVal == COMMAND_EXECUTION_SUCCESS_OPCODE) {
            return true;
        }
        return false;
    }
    /**
     *
     */
    private void closeConnection() {
        if (expect!=null) {
            expect.close();
        }
    }
    /**
     *
     * @param args
     */
    public static void main(String[] args) {
        String hostip="192.168.1.1";
      String usern="root";
      String pass="zychaa8zx62";
        String remote;
        String local;
        String server;
        String dest;
        String mask;
        String ip;
        String subnet;
        String broad;
        //String sim;
      Scanner input = new Scanner(System.in);

        /*System.out.println("----------------------- LOGIN DETAILS -------
-------------------");
        System.out.print("Enter Host IP: ");
        hostip = input.nextLine();
        System.out.print("Enter username: ");
        usern = input.nextLine();
        System.out.print("Enter password: ");
        pass = input.nextLine();*/


        System.out.println("-------------------------- GRE VPN ------------
------------------");
```

```
        System.out.print("Enter GRE server IP : ");
        server = input.nextLine();
        System.out.print("Enter GRE local  IP : ");
        local = input.nextLine();
        System.out.print("Enter GRE remote IP : ");
        remote = input.nextLine();
        //System.out.print("Enter sim IP: ");
        //sim = input.nextLine();

        System.out.println("------------------------ Static Route ---------
------------------");
        System.out.print("Enter destination IP :");
        dest=input.nextLine();
        System.out.print("Enter mask :");
        mask=input.nextLine();

        System.out.println("------------------------ LAN IP Setup ---------
------------------");
        System.out.print("Enter IP address :");
        ip=input.nextLine();
        System.out.print("Enter subnet mask :");
        subnet=input.nextLine();
        System.out.print("Enter broadcast IP :");
        broad=input.nextLine();



        SSHClient ssh = new SSHClient(hostip , usern , pass);
        List<String> cmdsToExecute = new ArrayList<String>();
        cmdsToExecute.add("ip  tunnel  add  gre3  mode  gre  remote  "+server+"
local any ttl 255");
        cmdsToExecute.add("ip link set gre3 up");
        cmdsToExecute.add("ip addr add "+local+" dev gre3");
        cmdsToExecute.add("ip route add "+remote+" dev gre3");
        cmdsToExecute.add("ip route del 0.0.0.0/0");
        cmdsToExecute.add("ip route add 0.0.0.0/0 via "+remote);
        cmdsToExecute.add("ip  route  add  "+dest+"/"+mask+"  dev  eth1.1  proto
static");
        //cmdsToExecute.add("ifconfig   br0   "+ip+"   netmask   "+subnet+"
broadcast "+broad);
        String outputLog = ssh.execute(cmdsToExecute);
        System.out.println(outputLog);
    }
}
```

Appendix H: IPSec TUNNEL INFORMATION AT END ROUTER

```
<Router>display ipsec sa
===============================
Interface: GigabitEthernet0/0/4
 Path MTU: 1500
===============================
  -----------------------------
  IPSec policy name: "jjj-policy"
  Sequence number  : 22
  Acl group        : 3001
  Acl rule         : 22
  Mode             : ISAKMP
  -----------------------------
    Connection ID     : 165
    Encapsulation mode: Tunnel
    Tunnel local      : 192.168.5.2
    Tunnel remote     : 192.168.3.2
    Flow source       : 192.168.6.0/255.255.255.0 0/0
    Flow destination  : 192.168.2.0/255.255.255.0 0/0
    Qos pre-classify  : Disable
    Qos group         : -

    [Outbound AH SAs]
      SPI: 840682851 (0x321bcd63)
      Proposal: AH-MD5-96
      SA remaining key duration (bytes/sec): 1887403380/2762
      Outpacket count       : 557
      Outpacket encap count : 557
      Outpacket drop count  : 0
      Max sent sequence-number: 557
      UDP encapsulation used for NAT traversal: N

    [Inbound AH SAs]
      SPI: 4014574010 (0xef4989ba)
      Proposal: AH-MD5-96
      SA remaining key duration (bytes/sec): 1887403380/2762
      Inpacket count        : 557
      Inpacket decap count  : 557
      Inpacket drop count   : 0
      Max received sequence-number: 557
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N

<Router>display ike sa conn-id 165
---------------------------------------
   Phase                    : Phase 2
   Peer name                : jjj
   Interface:               : GigabitEthernet0/0/4
   Connection ID            : 165
   IP address               : 192.168.3.2
   SA flag(s)               : RD
   Exchange type            : -
   NAT-traversal            : Disable
   UDP source port          : 500
   UDP destination port     : 500
   SA duration              : 3600 Seconds
   Policy name              : jjj-policy-22-22-0
   Phase 1 ConnID           : 155
   Encapsulation mode       : Tunnel
   Protocol 1               : AH
   Outgoing SPI             : 840682851
   Incoming SPI             : 4014574010
```

```
   DSCP value             : 255
---------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP

<Router>display ike peer

Number of IKE peers: 1


  Peer name       Exchange    Remote           NAT
                  mode        name             traversal
---------------------------------------------------------
  jjj             -                            Disable

<Router>display ike peer verbose

Number of IKE peers: 1

------------------------------------------
   Peer name                   : jjj
   IKE version                 : Version two
   Pre-shared-key              : test
   Proposal                    : 22
   Local ID type               : IP
   DPD                         : Disable
   DPD mode                    : Periodic
   DPD idle time               : 30
   DPD retransmit interval     : 15
   DPD retry limit             : 3
   Peer ID type                : IP
   Host name                   :
   Peer IP address             : 192.168.3.2(active)
   Host name                   :
   Peer IP address             :
   VPN name                    :
   Local IP address            : 192.168.5.2
   Local name                  :
   Remote name                 :
   NAT-traversal               : Disable
   PKI realm                   : NULL
   Inband OCSP                 : Disable
   Config-exchange-request     : Disable
   Config-exchange-set send    : Disable
   Config-exchange-set accept  : Disable
   Route accept any            : Disable
   Route preference            : -
   Route tag                   : -
------------------------------------------
<Router>dis ike proposal

Number of IKE Proposals: 2

-------------------------------------------
 IKE Proposal: 22
   Authentication method       : pre-shared
   Authentication algorithm    : SHA2-256
   Encryption algorithm        : AES-CBC-256
   DH group                    : MODP-1024
   SA duration                 : 86400
```

```
   PRF                         : PRF-HMAC-SHA2-256
-------------------------------------------

-------------------------------------------
 IKE Proposal: Default
   Authentication method      : pre-shared
   Authentication algorithm   : SHA1
   Encryption algorithm       : DES-CBC
   DH group                   : MODP-768
   SA duration                : 86400
   PRF                        : PRF-HMAC-SHA
-------------------------------------------
<Router>dis ipsec policy

===========================================
IPSec policy group: "jjj-policy"
Using interface: GigabitEthernet0/0/4
===========================================

    Sequence number: 22
    Security data flow: 3001
    Peer name    :  jjj
    Perfect forward secrecy: DH group 5
    Proposal name:  jjj-prop
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    Anti-replay window size: 32
    SA trigger mode: Automatic
    Route inject: None
    Qos pre-classify: Disable
    Qos group: -

<Router>dis ipsec proposal

Number of proposals: 1

IPSec proposal name: jjj-prop
 Encapsulation mode: Tunnel
 Transform         : ah-new
 AH protocol       : Authentication MD5-HMAC-96
```

Appendix I: IPSec TUNNEL INFO INSIDE L2-TUNNEL

```
<Router-A>display ipsec sa

===============================
Interface: GigabitEthernet0/0/5
 Path MTU: 1500
===============================

  -----------------------------
  IPSec policy name: "kkk-policy"
  Sequence number  : 22
  Acl group        : 3001
  Acl rule         : 22
  Mode             : ISAKMP
  -----------------------------
    Connection ID     : 174
    Encapsulation mode: Tunnel
    Tunnel local      : 192.168.3.2
    Tunnel remote     : 192.168.3.1
    Flow source       : 0.0.0.0/0.0.0.0 0/0
    Flow destination  : 0.0.0.0/0.0.0.0 0/0
    Qos pre-classify  : Disable
    Qos group         : -

    [Outbound AH SAs]
      SPI: 1687656161 (0x649796e1)
      Proposal: AH-MD5-96
      SA remaining key duration (bytes/sec): 1887436800/2734
      Outpacket count       : 0
      Outpacket encap count : 0
      Outpacket drop count  : 0
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: N

    [Inbound AH SAs]
      SPI: 620053493 (0x24f543f5)
      Proposal: AH-MD5-96
      SA remaining key duration (bytes/sec): 1887436800/2734
      Inpacket count        : 0
      Inpacket decap count  : 0
      Inpacket drop count   : 0
      Max received sequence-number: 0
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N
<Router-A>
<Router-A>
<Router-A>dis ik
<Router-A>dis ike sa
<Router-A>dis ike sa ver
<Router-A>dis ike sa verbose
<Router-A>dis
<Router-A>display ik
<Router-A>display ike sa
<Router-A>display ike sa ?
  conn-id    SA connection ID
  peer-name  IKE peer name, up to 15 characters
  phase      SA phase
  v2         Display the IkeV2 SA information
  verbose    Display detailed information
  <cr>       Please press ENTER to execute command
<Router-A>display ike sa co
<Router-A>display ike sa conn-id 174 ?
```

```
  <cr>  Please press ENTER to execute command
<Router-A>display ike sa conn-id 174
---------------------------------------
   Phase                    : Phase 2
   Peer name                : jjj
   Interface:               : GigabitEthernet0/0/5
   Connection ID            : 174
   IP address               : 192.168.3.1
   SA flag(s)               : RD
   Exchange type            : -
   NAT-traversal            : Disable
   UDP source port          : 500
   UDP destination port     : 500
   SA duration              : 3600 Seconds
   Policy name              : kkk-policy-22-22-0
   Phase 1 ConnID           : 173
   Encapsulation mode       : Tunnel
   Protocol 1               : AH
   Outgoing SPI             : 1687656161
   Incoming SPI             : 620053493
   DSCP value               : 255
---------------------------------------

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP

<Router-A>
<Router-A>
<Router-A>
<Router-A>
<Router-A>
<Router-A>dis ik
<Router-A>dis ike pee
<Router-A>dis ike peer

Number of IKE peers: 1


  Peer name       Exchange    Remote           NAT
                  mode        name             traversal
---------------------------------------------------------
  jjj             -                            Disable

<Router-A>
<Router-A>
<Router-A>
<Router-A>dis ike peer ve
<Router-A>dis ike peer verbose

Number of IKE peers: 1

------------------------------------------
   Peer name                    : jjj
   IKE version                  : Version two
   Pre-shared-key               : test
   Proposal                     : 22
   Local ID type                : IP
   DPD                          : Disable
   DPD mode                     : Periodic
   DPD idle time                : 30
   DPD retransmit interval      : 15
```

```
   DPD retry limit             : 3
   Peer ID type                : IP
   Host name                   :
   Peer IP address             : 192.168.3.1(active)
   Host name                   :
   Peer IP address             :
   VPN name                    :
   Local IP address            : 192.168.3.2
   Local name                  :
   Remote name                 :
   NAT-traversal               : Disable
   PKI realm                   : NULL
   Inband OCSP                 : Disable
   Config-exchange-request     : Disable
   Config-exchange-set send    : Disable
   Config-exchange-set accept : Disable
   Route accept any            : Disable
   Route preference            : -
   Route tag                   : -
------------------------------------------

<Router-A>
<Router-A>
<Router-A>
<Router-A>
<Router-A>dis
<Router-A>display ike
<Router-A>display ike pro
<Router-A>display ike proposal

Number of IKE Proposals: 2

-------------------------------------------
 IKE Proposal: 22
   Authentication method       : pre-shared
   Authentication algorithm    : SHA2-256
   Encryption algorithm        : AES-CBC-256
   DH group                    : MODP-1024
   SA duration                 : 86400
   PRF                         : PRF-HMAC-SHA2-256
-------------------------------------------

-------------------------------------------
 IKE Proposal: Default
   Authentication method       : pre-shared
   Authentication algorithm    : SHA1
   Encryption algorithm        : DES-CBC
   DH group                    : MODP-768
   SA duration                 : 86400
   PRF                         : PRF-HMAC-SHA
-------------------------------------------

<Router-A>
<Router-A>
<Router-A>
<Router-A>
<Router-A>dis ips
<Router-A>dis ipsec po
<Router-A>dis ipsec policy

===========================================
IPSec policy group: "kkk-policy"
```

```
Using interface: GigabitEthernet0/0/5
===========================================

    Sequence number: 22
    Security data flow: 3001
    Peer name    :  jjj
    Perfect forward secrecy: DH group 5
    Proposal name:  kkk-prop
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    Anti-replay window size: 32
    SA trigger mode: Automatic
    Route inject: None
    Qos pre-classify: Disable
    Qos group: -
<Router-A>
<Router-A>
<Router-A>
<Router-A>dis ips
<Router-A>dis ipsec pro
<Router-A>dis ipsec profile
<Router-A>dis ipsec propo
<Router-A>dis ipsec proposal

Number of proposals: 1

IPSec proposal name: kkk-prop
 Encapsulation mode: Tunnel
 Transform         : ah-new
 AH protocol       : Authentication MD5-HMAC-96
```