ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.3

Smart City Tunneling

Chanchal V. Dahat[1], Ankita Patil[2], Ayushi Shahu[3], Aakansha Kamble[4], Diksha Ganar[5], Neha Fulzele[6], Pranali Khankule[7]
Assistant Professor[1], BE Student[2, 3, 4, 5, 6, 7]
Department of Electronics and Tele-Communication Engineering
Nagpur Institute of Technology, Near Fetri, Mahurzari, Nagpur, India

Abstract:
Service providers today are constantly seeking to offer multiple services on a single common infrastructure. For instance, it is desirable some times to provide transport services transparently to data traffic encapsulated over different network layers. Tunneling is a technique for encapsulating a packet or frame within another packet of the same or a different network layer. One of the motivations for tunneling is bridging various heterogeneous networks that use different protocols for communication. Tunneling is also used for providing private and secure communications over a publicly shared network this article investigate the interactions between different tunneling technologies in order to provide end –to-end virtual connectivity to end clients. Particularly, the article describe the technical details of the implementation of various layer 2 tunneling techniques in order to establish an end-to-end virtual connection service as a concatenation of services offered by the different network domains along the path between end users. Security is the most important factor to be considered while designing a network and lot of research has been done in this field. One of the most effective ways for granting secured access in an organization is use of VPN. VPN is a generic term used as a combination of network topologies/technologies to describe a communication network through the tunnel, otherwise unsecured or not trusted network. VPN transmits data by the means of tunnels. The most important principle in establishing security through VPN tunnel is by providing proper Authentication and data encryption. The proposed method provides advanced encryption and authentication by using MAC address as a key. Whenever a sender wants to send any data through tunnel after establishment of the connection, the MAC address of the receivers device is read by the encryption technique it use it as a key to encrypt data.

Key words: VPN, Encryption, Authentication, Mac and Tunneling.

I. INTRODUCTION

Virtual Private Networks (VPNs) enable companies to connect geographically dispersed offices and n private company networks, using the public internet as backbone. Specially, VPN service in the broadband data communication network is very important and necessary to take in users who want to specify group communication. VPN mechanism are needed which work over existing deployed backbones. Project smart city tunneling is about to create a private network over a public network. It will at lease line on a network connecting to nodes directly with each other. As we create a lease line environment over a public network we create a secure data line to our customer. Data of the company or user can travel securely in a network at a lowest cost. *A computer network is topologies where two are more systems are connected together to share or exchange data. There are various types of computer networks. Some of them are:*

- **LAN (Local Area Network):** LAN is a topology where devices are connected at a single area typically an individual building like office, computer labs etc.,
- **MAN (Metropolitan Area Network):** MAN consists of a computer networks which may cover a small region. A WAN is larger than a LAN.
- **WAN (Wide Area Network):** WAN occupies a large area, which may be non-restricting or covers unlimited region. consist of multiple smaller networks. The best example of WAN is internet.

B. VPN: VPN is a generic term used as a combination of network topologies/technologies to describe a communication network through the tunnel.

There are mainly three types of VPN:
1) PC to PC VPN
2) Remote VPN
3) LAN to LAN VPN

VPN: VPN is a generic term used for the secure transformation of data within a bound closed network of systems. PC-to-PC VPN is used to transfer /share the within the connected systems. In the remote VPN, the client access the private network work which locates in the remote location when the VPN client /server is connected the VPN server provide the resources for access. During the providing the access to each other (both the client and the server) they should be authenticated themselves.

Site-to-Site/LAN-to-LAN: The VPN in one location connects with the other VPN in another location. This type of VPN connects two different VPN a routed connection which is logically operates as the stickled wide area network. In the site to site VPN network, the client VPN has to authenticate itself for the secure VPN and the server also authenticate itself for mutual authentication

C. VPN Supports Two Types of Tunneling –

1) Voluntary
2) Compulsory

In the voluntary tunneling, the VPN client establishes the connection with the network provider simply called VPN server, for example like the dial up connections. Then the, the line connection is utilized. So that it creates a tunnel to particular VPN server. Here the client is responsible for managing compulsory tunneling the set up for connection. In the compulsory tunneling the server or the network providers responsible for managing the VPN to Setup tunnel. Here the VPN access server configures and creates a tunnel instead of the client.

D. Tunneling protocols used to establish VPN:

- Point to Point Tunneling protocol (PPTP)
- Layer 2 Forwarding Protocol (L2F)
- Layer 2 Tunneling Protocol (L2TF)

1) PPTP:

PPTP is a protocol which is built on top of the PPP (Point- to-point protocol) of OSI layer two protocols. PPP is a dialup protocol used to connect to the Internet and also multiprotocol. PPTP is used by remote users to access private network by first dialing into their local Internet Service Provider. By creating a virtual network PPTP connects to the target network for each remote client. PPP session is also allowed by the PPTP, with non-TCP/IP protocols to be tunneled through an IP network.

2) L2TP (Layer 2 Tunneling Protocol):

L2TP (Layer 2 Tunneling Protocol) which simple says as is a combination of Microsoft Point-to-Point Tunneling Protocol (PPTP) and Cisco Layer 2 Forwarding (L2F). L2TP can be used as a tunneling protocol to encapsulate PPP (Point-to-Point Protocol) frames to be sent over IP, X.25, and Frame Relay or ATM networks. Multiple connections are allowed through one tunnel. Like PPTP and L2F, L2TP operates on OSI layer two. Layer two VPN protocols encapsulate data in PPP frames and are capable of Non-IP protocols over an IP network.

E. IPSec in a Network Tunneling Mode:

1) Transport mode:

In the Transport mode, usually encrypted and/or authenticated is provided for only the payload of the IP packet.

2) Tunneling Mode:

In this tunneling mode, encryption and/or authentication is done for entire IP packet. It is then a new IP packet encapsulated with a new IP header.

II. EXISTING SYSTEM

In the protocols PPTP an L2F provides authentication by the password .But they doesn't provide the security to the payload. These two protocols PPTP and L2F are both used in L2TF protocol. The following figure shows the example representation of existing system use in VPNs and LANs.

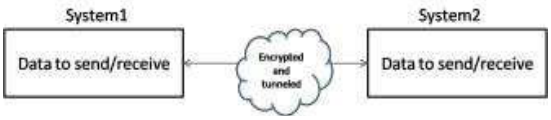

Figure.1. Example of existing system

The main contributions of this paper are:

- We provide proper authentication, integrity and confidentiality to the data before sending it.
- VPNs are a great way to maintain privacy and avoid transmitting sensitive data over public networks. Even though load times may increase with distance, they serve the purpose for which they were intended Privacy & Security.
- Secured connection can be created between two nodes
- Low cost service can be given to the common people.
- Data Transfer speed is High.

III. PROPOSED SYSTEM

The proposed system we can overcome the drawbacks of the existing system, for that we provide proper authentication, integrity and confidentiality to the data before sending it. Our proposed system is simply the client server model in which encryption and decryption is done in the same system itself. This following figure 1a shows the format of encryption and decryption.

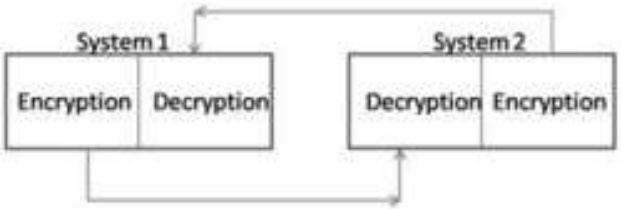

Figure.1. a: Client-server Encryption and Decryption process.

- In Proposed method, the data is protected by encryptions (preferably using receiver's MAC address as a key) which provide both encryption and authentication.
- Whenever a sender wants to send any data, the data is send through tunnel after establishment of connection with sever/host to which the sender needs to send. The MAC address of the receiver is used as a key for encryption technique to encrypt data.
- After Encryption tunneling is configured before sending it.
- Similarly after receiving cipher data by the receiver, he/she can decrypt the data by their own system MAC address to which the data is sent.

IV. METHODOLOGY

A. Architecture:

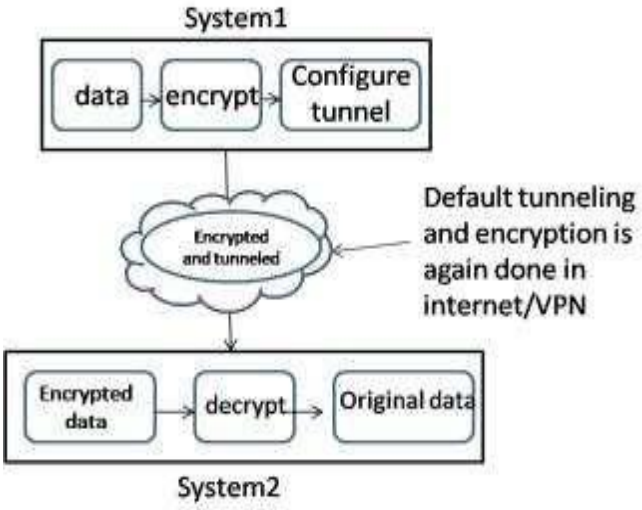

Figure.1b. overview of data transmission in proposed method

In this paper we are using the Rijndael Algorithm (Advanced Encryption Standard) for the encrypting of any data file format .The encrypted file or data of any format is then provided a tunnel configuration .So that we can provide the both encryption and tunneling before sending the file to other system. If we send data through the internet or VPN, there the policies of that transfer provide some security to the cipher file which we sent. So that the data is full secured by our side (client/server) and also protected during transfer. So that the data which we are going to send or receive is fully secured. If we encrypt the file using the key of the receivers MAC address, the user can easily decrypt the file using his/her own systems MAC address. If the key given wrongly during decryption the file shows as decrypted file successfully but generates a corrupted or modified data format file. Hence

without the proper key data is decrypted but with improper data. Unless the proper key is not given the data doesn't shown as the original data (before encrypted data).

B. Advance Encryption Standard

The Advanced Encryption Standard (AES) is a Symmetric block cipher intended to replace DES for commercial applications which was published by NIST (National institute of standards and Technology) in 2001.It uses a key size of 128,192 or 256 bits and a 128-bit block size , this is a standard symmetric block cipher which is based on the Rijndael algorithm. The AES algorithm used three different key lengths; these three are referred to as "AES-128", "AES-192" and "AES-256".Mainly four different steps are involved in the AES algorithm, which are executed in a sequential manner and forming rounds. Depending upon the key lengths the rounds number is varying. The below Fig: 2 shows the parameters of the AES algorithm.

B. Preferable key used for Encryption:

The key used in AES Algorithm for encryption is preferably MAC address of the receiver. So that the data is encrypted with the receivers MAC address. The receiver can decrypt by using his own system MAC address. We have a many tools and method to find the MAC address of the receiver system which is connected to our system. Instead of that we can simply find MAC address of the other systems connected to our system by using the command prompt. In the command prompt give the command line as, Arp –a. This command gives the MAC addresses of system, IP address of system with the type of connection they are connected.

C. Tunnel configuration:

After the encryption of our data, while sending data, the tunnel is configure. In the tunnel the sending data is encrypted In the tunnel the sending data is encrypted to provide security to data. We have much number of ways to configure the tunneling. Some of the ways to configure tunneling is by using CISCO networks, Cyberoam networks, Paloalto networks and simple tools like putty, etc. In the cyberoam and paloalto networks we have different types of tunneling which we have to make use of it and conFig. The tunnels. We can also define our own policies in these networks. Putty is a simple opensoure application tool which is used for configuration of the tunnel. This tool is reliable n feasible to every user for their individual works also.

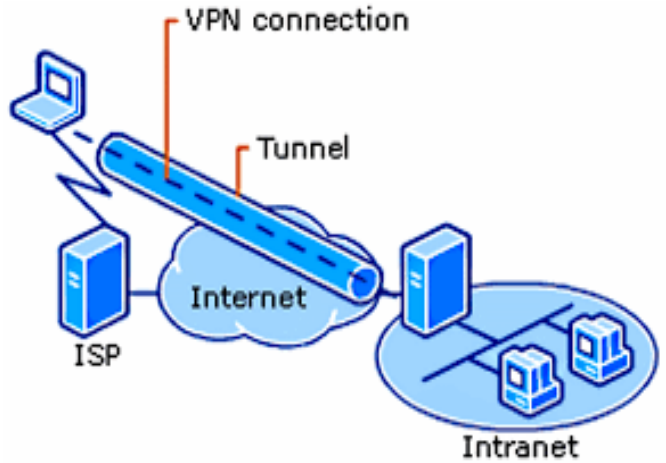

Figure.1c. data transmission in tunnel

Tunneling is a technique that enables remote access users to connect to a variety of network resources (Corporate Home Gateways or an Internet Service Provider) through a public data network. In general, tunnels established through the public network are point-to-point (though a multipoint tunnel is possible) and link a remote user to some resource at the far end of the tunnel. Major tunneling protocols (i.e.: Layer 2 Tunneling Protocol (L2TP), Point to Point Tunneling Protocol (PPTP), and Layer 2 Forwarding (L2F)) encapsulate Layer 2 traffic from the remote user and send it across the public network to the far end of the tunnel where it is de-encapsulated and sent to its destination. The most significant benefit of Tunneling is that it allows for the creation of VPNs over public data networks to provide cost savings for both end users, who do not have to create dedicated networks, and for Service Providers, who can leverage their network investments across many VPN customers. To understand a particular protocol stack imposed by tunneling, network engineers must understand both the payload and delivery protocol sets. As an example of network layer over network layer, Generic Routing Encapsulation (GRE), a protocol running over IP (IP protocol number 47), often serves to carry IP packets, with RFC 1918 private addresses, over the Internet using delivery packets with public IP addresses. In this case, the delivery and payload protocols are the same, but the payload addresses are incompatible with those of the delivery network. It is also possible to establish a connection using the data link layer. The Layer 2 Tunneling Protocol (L2TP) allows the transmission of frames between two nodes. A tunnel is not encrypted by default, it relies on the TCP/IP protocol chosen to determine the level of security. Data encryption of payload being transmitted over a public network (such as the Internet) connection, thereby providing VPN functionality. IP sec has an end-to-end Transport Mode, but can also operate in a tunneling mode through a trusted security gateway.

V. RESULT:

The text data format is encrypted; other data files like image, PDF, music format like mp3, mp4, etc are corrupted after encryption. By using the tunnel configuration, the encrypted file is again encrypted during tunneling and tunneled. So that the data is fully secured. If we send through the internet there the data is tunneled again so that double tunnel is provided and indirectly encryption also done to the encrypted data. Hence the data is fully secured.

VI. CONCLUSION

With the help of Proposed System, there is a secure data transmission by using the MAC address as a key for Encryption and tunneling is configure. The most important principle in establishing security through VPN tunnel is by providing proper Authentication and data encryption. The project is a prototype for future. It will help middleclass IT companies to grow up and expand their Infrastructure at low cost and secure network.

VII. REFERENCES

[1]. "Extending IP & Ethernet" published in Technical conference & Exhibition, 143rd.

[2]. N. Borisov, I. Goldberg & D. Wagner, (2014) "Intercepting Mobile Communications: The Insecurity of Proceedings of the Seventh Annual International conference on Mobile communication and networking.

[3]. Ferguson, P. and Huston, G,. "what is VPN ? ", Revision, April 1998.

[4]. Calhoun, P. et al., "Tunnel Establishment Protocol", Internet Draft, March 1998.

[5]. Townsley, W. et al, "Layer Two Tunneling Protocol 'LT2P'", RFC2661, August 1999.

[6]. Singh, A.K.; Samaddar, S.G.; Misra, A.K."Enhancing VPN security through security policy management", 2012.

[7]. http://csrc.nist.gov/archive/aes/rijndael/Rijndaelammended.

[8]. Cryptography and network security, W.Stallings Chen Fei Wu Kehe ; Chen Wei ; Zhang Qianyuan:"

[9] VPN security -2008 © The Government of the Hong Kong Special Administrative Region