RESEARCH PAPER | Engineering | Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

Performance of Two Dimensional Tunneling for Secure Data Transmission in Vpn

KEYWORDS: Tunneling, Authentication, BGP, Virtual Points, Encapsulation.

Jayanthi Gokulakrishnan
Research Scholar, Sathyabama University, Chennai, India.

V. Thulasi Bai
Vice-Principal & Dean, Department of ECE, Prathyusha Institute of Technology & Management, Chennai, India.

ABSTRACT *A VPN is a private network that uses a public network "usually the Internet" to connect remote sites or users together. VPNs provide the ability for two offices to communicate with each other in such a way that it looks like they're directly connected over a private leased line Instead of using a dedicated line for the communication between two parties across the globe, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. One of the most important solutions to viruses and hackers threats is VPN that makes the network between companies and users secured; it is also authenticated and encrypted for security. The communication between the end to end nodes takes place in three phases: tunneling phase, decryption phase and authentication phase. In the tunneling phase, the data is tunneled with a special identification code of nodes and sends to authenticated nodes. All the intermediate nodes once again tunnel the nodes and send towards the destination. The number of tunneling increases with the increase of point to point communication. Intermediate VPN allows decode the data structure to a certain range. Thus this technique efficiently allows the packet to be transmitted with ensured security. In this paper, the performance of secure tunneling is evaluated with certain attributes like block size, tunneling delay, throughput, packet loss etc. with respect to Border Gateway Protocol.*

1. INTRODUCTION

Virtual Private Networks (VPNs) have become an easy way of securing communications over the internet. VPN services are the fundamental services of distributed systems over the internet. The working of VPN is transparent to the end-users. The end-users are connected to a local network and they are interconnected by the public internet. The end-users interact with each other through gateways. Different network topologies co-exist in VPN. Each gateway maintains information about the local hosts belonging to the VPN and the peer gateways that manage remote LANs.

A VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and other information transmitted between two endpoints. Because a VPN can be used over existing networks such as the Internet, it can facilitate the secure transfer of sensitive data across public networks [4]. A private network is composed of computers owned by a single organization that share information specifically with each other. They're assured that they are going to be the only ones using the network, and that information sent between them will (at worst) only be seen by others in the group. The typical corporate Local Area Network (LAN) or Wide Area Network (WAN) is an example of a private network [9]. The line between a private and public network has always been drawn at the gateway router, where a company will erect a firewall to keep intruders from the public network out of their private network, or to keep their own internal users from perusing the public network. A VPN is an example of providing a controlled connectivity over a public network such as the Internet. VPNs utilize a concept called an IP tunnel—a virtual point-to-point link between a pair of nodes that are actually separated by an arbitrary number of networks. The virtual link is created within the router at the entrance to the tunnel by providing it with the IP address of the router at the far end of the tunnel. Whenever the router at the entrance of the tunnel wants to send a packet over this virtual link, it encapsulates the packet inside an IP datagram. The destination address in the IP header is the address of the router at the far end of the tunnel, while the source address is that of the encapsulating router. VPN transmits data by means of tunneling. Before a packet is transmitted, it is encapsulated (wrapped) in a new packet, with a new header. This header provides routing information so that it can traverse a shared or public network, before it reaches its tunnel endpoint. This logical path that the encapsulated packets travel through is called a tunnel. When each packet reaches the tunnel endpoint, it is "decapsulated" and forwarded to its final destination. Both tunnel endpoints need to support the same tunneling protocol [6].

1.1Advantages of Virtual Private Networks

VPNs allow the users to use the public Internet to securely connect remote offices and remote employees at a fraction of the cost of dedicated, private telephone lines. There are two major uses for VPNs. The first is to connect two or more geographically separated networks, such as those at a main office and a remote branch office. The second is to allow employees or authorized users to access a network from a remote PC, such as laptop or home computer. Both of these uses permit access to protected network resources by authorized users. The technologies provide solutions geared towards the unique requirements of each uses [7][8]. A well-designed VPN can greatly benefit a company. For example, it can: Extend geographic connectivity, Improve security, Reduce operational costs versus traditional WAN VPN, Reduce transit time and transportation costs for remote users, Improve productivity, Simplify network topology, Provide global networking opportunities, Provide telecommuter support, Provide broadband networking compatibility, Provide faster return on investment (ROI) than traditional WAN. The important features of a VPN are: Security, Reliability, Scalability, Network management and Policy management.

The paper is organized as follows: Security issues in VPN are discussed in Section 2. Section 3 contains Literature Review. The proposed architecture of VPN is described in Section 4. Simulation environment and the results are described in Section 5. Section 6 contains conclusion.

2. SECURITY ISSUES IN VPN

The security of the VPN can be measured with the following parameters:

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

Authentication: Verifies that the packet received is actually from the claimed sender.

Confidentiality: IPSec can ensure that data cannot be read by unauthorized parties [5]. This is accomplished by encrypting data using a cryptographic algorithm and a secret key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity: IPSec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication: Each IPSec endpoint confirms the identity of the other IPSec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host [5].

Replay Protection: The same data is not delivered multiple times, and data are not delivered grossly out of order. However, IPSec does not ensure that data is delivered in the exact order in which it is sent.

Traffic Analysis Protection: A person monitoring network traffic does not know which parties are communicating, how often communication is occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control: IPSec endpoints can perform filtering to ensure that only authorized IPSec users can access particular network resources. IPSec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

Some other threats observed from the users' point of view as given below [6]:
VPNs carry sensitive information over an insecure network. The users generally trust the VPN to keep the information secure, which is understandable because that is what the VPN is designed to do. Because of this trust, the users will transfer sensitive data without using additional encryption, and use protocols that transmit authentication credentials in the clear.

Remote Access VPNs often allow full access to the internal network. Many organizations configure their remote access VPNs to allow full access to the internal network for VPN users. This means that if the VPN is compromised, then the attacker gets full access to the internal network too. VPN traffic is often invisible to IDS monitoring. If the IDS probe is outside the VPN server, as is often the case, then the IDS cannot see the traffic within the VPN tunnel because it is encrypted. Therefore if a hacker gains access to the VPN, he can attack the internal Systems without being picked up by the IDS. As more organizations install firewalls, more Internet servers onto the DMZ, automatically patch servers etc., the VPN becomes a more tempting target.

3. LITERATURE REVIEW

A secure design for network and system in a windows environment using the latest technology is proposed in [3]. The security of networks always faces new potential threats as hackers and viruses advance. The design shows how the network can be more secure by encrypting the sending data using internet protocol security between the user and server. The purpose of network security is to provide availability, integrity, and confidentiality. The design shows how the network can be more secure by encrypting the sending data using internet protocol security between users and servers. The purpose of network security is to provide availability, integrity, and confidentiality. This procedure does not tackle the technologies adaptance according to the requirement of the network. If a number of VPN is increasing this method is not able to provide a suitable solution.

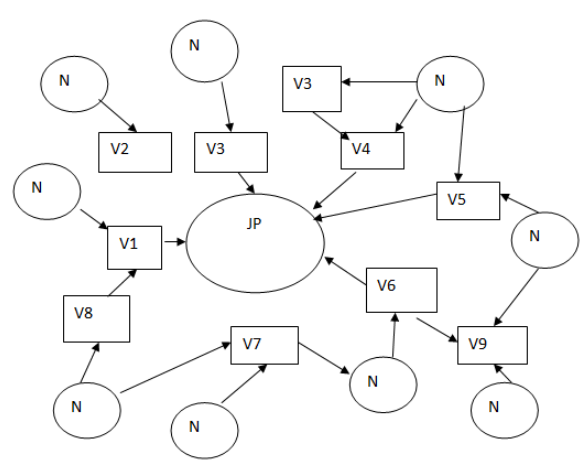
The vulnerabilities found in VPN using IPSec and a set of policies as a Defensive measure are suggested in [1]. The policies suggested applied to implementations of VPN that are directed through an IPSec concentrator and to all company' s employee, contractors, consultants, temporaries and other workers including all personnel affiliated with the third parties utilizing VPNs to access the company' s network. The attacks described in the paper puts all VPNs at risk that uses pre-shared keys for authentication and accepts VPN connections from anywhere like access for traveling users. The authors have also suggested policy for to provide guidelines for remote access IPSec virtual private network connections to the company's corporate network. But, the proposed method is unable to describe the model in a multi hop or multi VPN scenarios. Timing concept always needs a synchronized method which is costly.

A new type of fusion encryption protocol for VPN data encryption and key management is proposed in [2]. In this approach the VPN server is the trusted authority. The VPN client initiates the request; the VPN server gives the key value. Using the key value VPN client securely encrypt data with the help of AES-Rijndael. Then the key value is encrypted using receiver's public key with the help of RSA. Then these encrypted values integrated together and send to the receiver. The receiver using its private key and RSA identifies the original key value. Using original key the encrypted data is decrypted with the help of AES-Rijndael. The main advantage of this method is that it takes much lesser time when compared to normal encryption with secure key transformation process. Compared to the previous approach, the proposed approach is more secure to transfer sensitive information through the public network. This method does not describe mutual data transmission in a soft manner.

4. PROPOSED TUNNELING METHOD

The data to be transmitted is stored in the form a single dimensional array. The data packets contain the address of the destination node. Any data which is transmitted goes through upstream and downstream processes. In the upstream process, the data is transmitted to the junction point through virtual points. The downstream process consists of transmission of data from the junction point to the destination node. The data transmitted passes through one or more than one virtual points before it reaches the destination node through the junction node. During upstream process, the data is encrypted as it goes through various virtual points with their own keys. During downstream process, the encrypted data is decrypted till the receiver receives the data.

The architecture of the VPN is given below:



Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

Fig. 1 Architecture of VPN

In the above fig.1, N denotes nodes, V denotes virtual points and JP denotes junction point. When the data is transmitted to the destination node, it is transmitted through various virtual points. When the data reaches a virtual point, it checks the destination address in the data packet. If the destination address does not match with its address, it passes the data packet to the next virtual point. This process is continued till it reaches its destination address.

The flow chart of the procedure is given below:

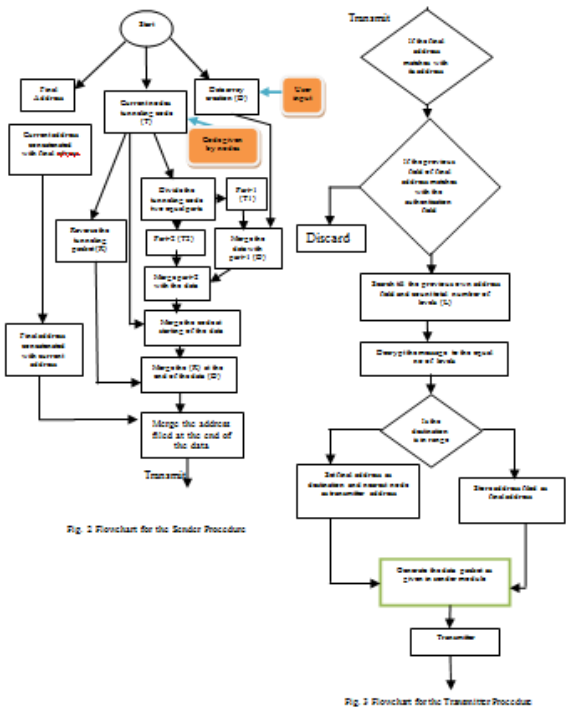


Fig. 3 Flowchart for the Transmitter Procedure

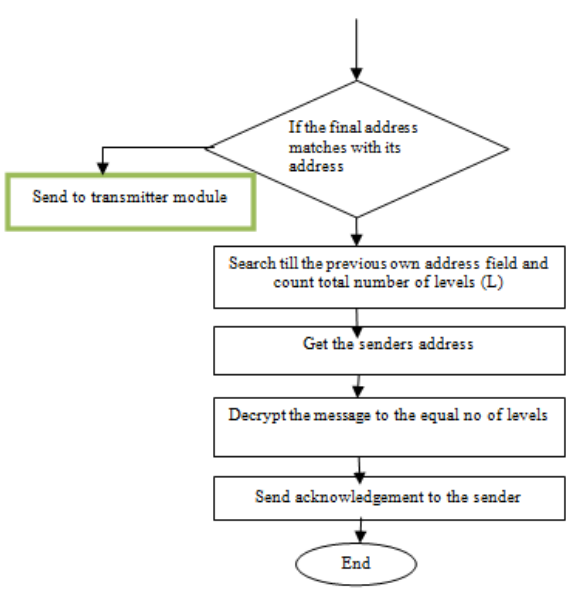


Fig. 4 Flowchart for the Receiver Procedure

5. SIMULATION RESULTS

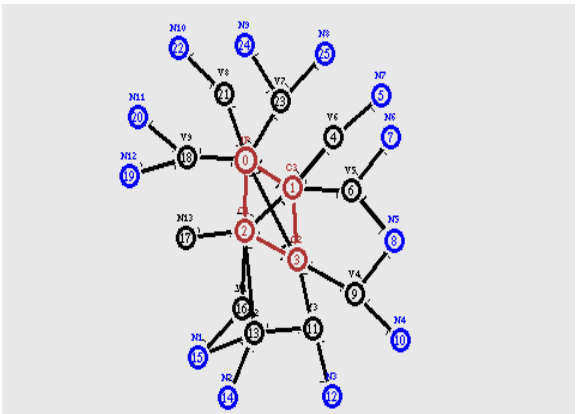


Fig. 5 Simulation Topology

5.1Simulation Setup

This section deals with the experimental performance evaluation of our proposed system through simulations. In order to test our protocol, the Network simulator 2 (NS2) is used. NS2 is a general-purpose simulation tool that provides discrete event simulation of user defined networks. NS-BGP extension 2.0 of ns-2.33 was used for simulating the BGP architecture. The experimental setup is shown in the figure 11. The simulation setup consists of 10 Autonomous systems (AS) nodes which are connected to each other. Each AS has separate network prefix addresses ranging from 10.0.0.1 to 10.0.9.1. The link bandwidth is 10Mb and link delay is 20ms. BGP agent is attached to each AS connected with neighbor AS as shown in the figure 11. CBR traffic is used with packet size 100 bytes. The traffic rate is varied from 0.5Mb to 2.5Mb. AS 8 is considered as an attacker which performs prefix hijacking attack against the path AS9 to AS3.

5.2 Simulation Results

5.2.1 Based On Attackers

Initially attackers performing prefix hijacking attacks are deployed. The attackers are varied from 1 to 5 and the percentage of compromised nodes is evaluated. The result of the simulation is given in fig. 6. It is observed that the two dimensional tunneling for data transmission (TDTDT) has less percentage of compromised nodes, because of its shell like structure.

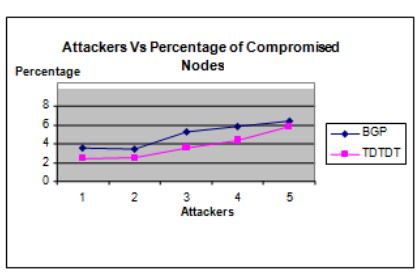


Fig. 6 Attackers vs. % of Compromised Nodes

5.2.2 Based on Rate

In this experiment, the data sending rate is varied from 0.5Mb to 2.5 Mb. The packet loss ratio is measured. Fig.7 shows that packet loss ratio increases when the rate is increased. From the figure, it is seen that the TDTDT has very low packet loss ratio when compared to normal BGP scenario.

Volume : 3 | Issue : 9 | Sept 2013 | ISSN - 2249-555X

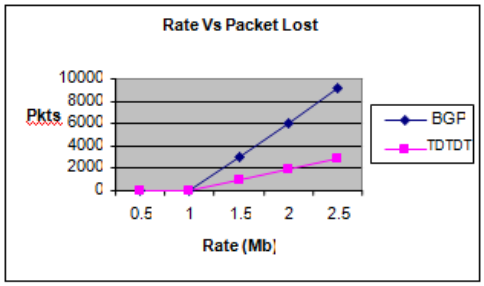


Fig. 7 Rate vs. Packet Lost

5.2.3 Based on Block Size

Packet delivery ratio is the attributes considered against block size for the performance evaluation of TWTDT.

Fig.8 show that packet delivery ratio (PDR) increases when the size is increased. From the figure, it is seen that the TDTDT has high PDR when compared to normal BGP VPN scenario.

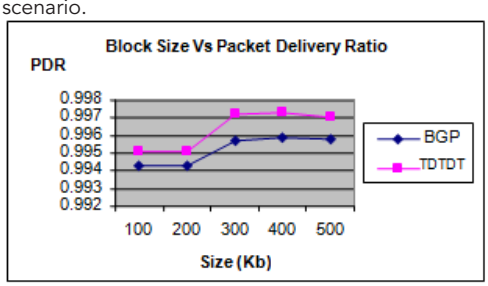


Fig. 8 Block Size vs. PDR

6. CONCLUSION

It is observed and verified from the simulation results that the two dimensional tunneling for data transmission (TDTDT) is a secure method for data transmission when compared to the traditional tunneling method employed in the border gateway protocol (BGP). This method ensures that the data is transparent to the outside attackers and users. The data can be decrypted by the authenticated user only. Since the method employs shell for data security, breaking of shell is very difficult for the attackers. The experimental results show that TDTDT performs better in all the attributes considered for the simulation than the traditional tunneling method employed by BGP.

REFERENCE

Byeong-Ho Kang and Maricel O. Balitanas," Vulnerabilities of VPN using IPSec and Defensive Measures", International Journal OF Advanced Science and Technology Volume 8, July, 2009. | | [2] M.Sreedevi, Dr. R. Seshadri," An innovative kind of security protocol using fusion encryption in virtual private networking", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012. | | [3] Seifedine Kadry, Wassim Hassan," Design and implementation of system and network security for an enterprise with worldwide branches, Journal of Theoretical and Applied Information Technology,2008 | | [4] Sheila Frankel, Paul Hoffman Angela Orebaugh & Richard Park," Recommendations of the National Institute of Standards and Technology", NIST Special Publication 800-113. | | [5] Sheila Frankel Karen, Kent Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey & Steven R. Sharma," Guide to IPSec VPNs", NIST Special Publication 800-77. | | [6] The Government of the Hong Kong Special Administrative Region VPN SECURITY," February 2008. | | [7] Benefits of Using VPN Technology", 1999 technologies, Inc. an eSoft company. | | [8] Jeff Tyson, "How Virtual Private Networks Work", http://computer.howstuffworks.com/ | | [9] Charlie Scott, Paul Wolfe, Mike Erwin," Virtual Private Networks, Second Edition" O'Reilly Second Edition January 1999. | |