A Topology–Aware Reliable Routing Protocol for Internet Security in Virtual Private Network

Jayanthi Gokulakrishnan
Research Scholar, Sathyabama University
Panimalar Institute of Technology
Chennai, India

V. Thulasi Bai
Phd,Professor & Dean,
Prathyusha Institute of Technology & Management
Chennai, India

ABSTRACT
Most of the Virtual Private Network (VPN) suffers from security related and overhead problems. During the inter domain routing, the conventional protocols require each gateway to resend its routing table periodically to all its neighbors thus increasing the delay. Since VPNs carry sensitive information over an insecure network, the traffic in this network has to be transmitted reliably and securely. In this paper, we propose a topology aware reliable routing protocol for inter-domain routing in VPN which securely transfers the data. By simulation results, we show that our proposed protocol is better than the traditional routing protocols of VPN.

Keywords
VPN, Topology-aware Protocol, Gateway, Authentication.

1. INTRODUCTION

A network which merges the usage of the public and the private networks and uses security software for the purpose of compressing, encrypting and masking the digital packets that are being transmitted in the network is called as virtual private network (VPN). VPNs are configured to be private national or international networks to its customer by the telecommunication carriers even when it shares its backbone trunks with additional customers [1]. In VPN, the communication between the two end users is maintained such that it appears as if the source end is directly linked to the destination end over a concealed leased line. The private network, VPN uses the public network such as internet to link the remote locations with the users. Unlike the other networks which use the devoted, real world link for communication, the VPN makes use of the "virtual" links from the private network of the company which routes through the internet to the company employee or the remote location [2]. A virtual private network (VPN) is basically a communication network which is devoted and consists of several ventures that are situated over a range of location and linked to each other through some open communication network such as internet. A VPN is called as the corporate intranet when every location of the VPN is in possession of the same venture. The VPN is called as extranet if the sites of the VPN are in possession of different ventures. The paper is organized as follows: Section 1 presents the introduction about VPN. Section 2 deals with the related work. In Section 3, we present our proposed work. Section 4 deals with the new protocol proposed. Section 5 presents the simulation setup and results. Finally, Section 6 contains the conclusion.

2. RELATED WORK

E. Ramaraj et al [3] has focused on single trusted authority which uses public key cryptography RSA in EAP instead of multiple trusted authorities and also AES-Rijndael stream cipher algorithm instead of RC4 for MPPE. A new type of hybrid encryption technique using AES-Rijndael for encryption and decryption is proposed and RSA is used for key management.

Christoforos Ntantogian et al [4] has proposed a security protocol that provides mutual authentication between a user and a WLAN that the first tries to connect to, and deploys a mobile Virtual Private Network (VPN) that protects the user's data conveyed over the wireless network. For the user authentication as well as for the initialization of the VPN and the related key agreement, the EAP-SIM encapsulated within the Internet Key Exchange version 2 (IKEv2) is proposed. The deployed VPN, which is based on IPSec, ensures confidentiality, source authentication and integrity of the data exchanged over the WLAN. At the same time, the user has been subscribed to the 3G-network for charging and billing purposes using the legacy EAP-SIM authentication protocol. The established VPN can seamlessly operate and continuously provide security services as the mobile user moves and roams, materializing the notion of mobile VPN. The proposed security protocol eliminates the required enhancements to the current network infrastructure and operates transparently to the existing network functionality. The main drawback of the proposed protocol is that its deployment may increase the computational overhead of the involved entities compared to the pure EAP-SIM.

Lookman Fazal et al [5] has demonstrated a security issue with such deployments, which is referred to as the hidden wireless router vulnerability. This vulnerability is inherent in the VPN-based wireless LAN architecture, and leads to unsuspecting clients becoming conduits for an attack, exploiting features readily available in popular operating systems like Windows and Linux. The attack scenario and possible solutions for both detecting and locating such hidden wireless routers is described. The solutions include a range of possibilities stretching from purely passive to active probing methods, and Access Point-based solutions.

Vassilis Prevelakis et al [6] has proposed the use of a special purpose drop-in firewall/VPN gateway called Sieve, which can be inserted between the mobile workstation and the network to provide individualized security services for that particular station. Sieve is meant to be used like an external modem. The user only needs to plug it in. Its existence is transparent to the user, thus requiring no modification to the workstation configuration.

3. PROPOSED WORK

Most of the VPN has security related and overhead problems. During the inter domain routing, the conventional RIP [7] requires each gateway to resend its routing table periodically to all its neighbors thus increasing the delay in database updation whereas in intra domain routing, the conventional OSPF[8] and IS-IS[9] protocol used requires built-in mechanisms to handle in-order and reliable message delivery. Also it cannot solve the link level

indicator consistency problem without the use of the sequence numbers, periodic link-state refreshments, or link-state flooding.
Hence, in this paper we develop a routing protocol in which the communication at the inter domain level is carried out at an efficient way and the data transmission in the network is encapsulated. The routing design has a topology learning protocol which offers a fundamental technique for determining the routes in the domain level and also the route failures and attacks to the users. In a user's upstream, the provider-level route sets are distributed by the protocol and then by the use of the link level indicator messages, the users are informed about the conditions of the dynamic network. On the basis of the messages heard from the neighbors, the topology status is updated by the protocol.
The protocol runs amid the domain border routers and its operation is performed outer to the Core of the internet. The upstream is propagated to the users and inter-domain forwarding entries are established for the gateway by the protocol. In contrast to the OSPF and IS-IS, inbuilt mechanisms are not required by this protocol to provide in-order and reliable message delivery. On the other hand, it transfers the messages in-order and reliably using the failure free secure shortest path.

4. TOPOLOGY-AWARE RELIABLE ROUTING PROTOCOL

4.1 System Design

In our work, we develop an inter-domain routing protocol for VPN which transfers the packet on demand with high reliability and security. The system architecture consists of the central unit called as the core, the VPN gateway and the nodes. Initially, within the network a core region is identified which refers to any common network segment in a delivery path that has been determined unfit for transporting unencrypted traffic generated by edge networks. So it is suitable only for the transfer of the encrypted messages. The VPN gateway maintains the information about its surrounding nodes and directs the packet accordingly through the network. In order to direct the packet efficiently, all of the VPN gateways register itself to a Junction Point (JP) which is situated within the core. Once the VPN gateway is registered at the JP then the gateway gets information about all the other gateways that are connected to the core.
The nodes are the edge networks which encrypt the packets before transmission, across the network. The path for the transfer of the packet can be divided into three segments. The packet is transmitted through upstream at the source, core and then the downstream at the destination. A source user's upstream has an "uphill" segment consisting of a sequence of the sender's providers i.e., the upstream, is a small region of the Internet, consisting of only a user's direct and indirect providers, and their peering links. The downstream has a "downhill" segment which consists of a sequence of the receiver's providers. A sender's upstream contains the uphill segment of a route, and the destination's downstream contains the downhill part.
The network architecture is given in the fig.1. It consists of a core region with a junction point, 14 nodes and 9 VPN gateways. In this fig, node 3 sends the packet to node 13. The up graph at the source for the transmission of the packet consists of the uphill segment which can be 3-V1-core or 3-4-V2-core or 3-4-V3-core. Through the core the packet is transmitted in the encrypted form. At the receiver side, the packet is transmitted along the downhill graph. The downhill segment in the downhill graph can be core-V8-13 or core-V9-14-13.

4.2 Gateway Authorization

For each pair of edge network that wish to communicate, a VPN tunnel must be established between them. This requires that the VPN gateway at the source know the core address of the destination. To make all nodes available to each other, each VPN gateway needs to be configured with a mapping between core addresses and node address in addition to maintaining key parameters for each node. A VPN link has to be developed between the two edge nodes that want to communicate with each other. A table containing the core address, the nodes address and the key parameters for every node is maintained at every VPN gateway in order to allow communication between all the nodes possible.
Within the network, every VPN gateway registers itself to the JP. As soon as the VPN gateway gets registered at the JP, it receives a list of information about the other VPN gateways that are connected to the core. Based on this information, the VPN gateway at the source end can easily determine the best path towards any other destination VPN gateway. Within the core, a Junction Point (JP) maintained by the network is responsible for the efficient functioning of the gateway. Initially the gateway maintains a routing table which consists of information regarding the nodes attached to it. The VPN gateway also maintains the information related to all the other gateways attached to the core in its table

4.3 Route Discovery

For the upstream discovery by the user, a protocol called as the Topology Learning Protocol (TLP) is developed. In a TLP, two agents are used: path vector agent and policy based link level indicator agent. The path vector agent is used for the distribution of the provider level path set in the upstream of the user. The information about the direct and the indirect providers for the user, along with the transmission paths established by these providers is offered by the path vector agent. The dynamic network conditions of the user are informed by the policy-based link level indicator agent. For route discovery, initially the tier-1 providers will advertise itself to its customer, and then the customers will attach themselves and advertise this new route to its customers.
In the example of Figure 1, a user domain 3 learns from TLP that it can use three routes to reach the Core: 3-V1-core or 3-4-V2-core or 3-4-V3-core. In a path, every node will be a direct provider or an indirect provider. In TLP, the user is given information about the dynamics of the network by the link level indicator agent. The limit up to which the propagation of the link level indicator message can be allowed and also the selection of the neighbor which has to be exposed to the adjacent domain-level link. With this policy, a user domain 3 only learns the domain-level links on his up-graph, which includes 3 to V1, 3 to 4, V1 to core, 4 to V2, 4 to V3, V2 to core and V3 to core.

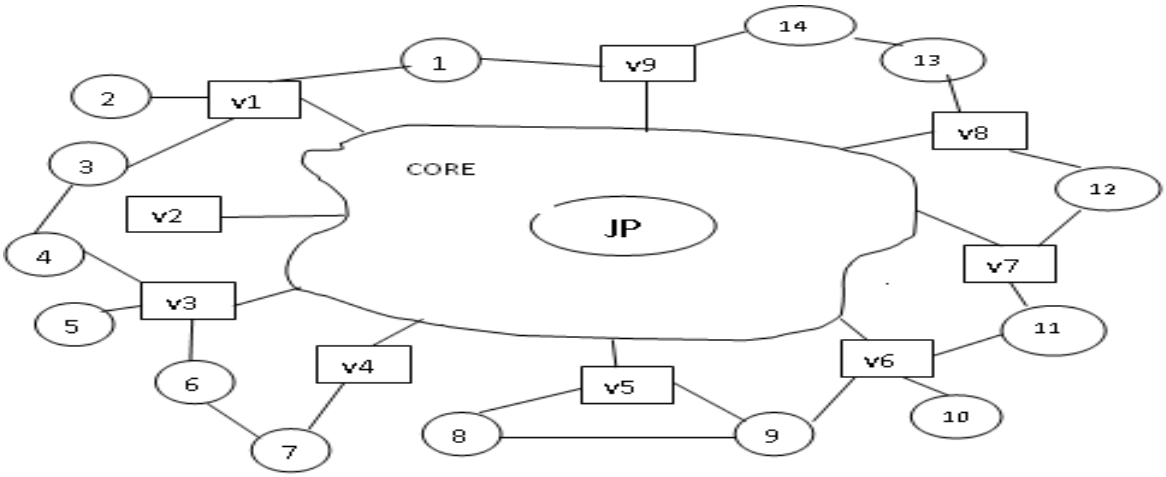

Fig.1. Network Architecture of VPN

By combining the upstream and the downstream routes together, the sender node at the source can establish a complete path from the source node to the destination. A classic domain level route is "error-free". For a route, the upstream at the source consists of the "uphill" segment and the downstream at the receiver end consists of the "downhill" segment. TLP provides the source all the required information about the uphill segment. The information about half the route towards the destination is obtained from the lookup service i.e., the Name-to-Route Lookup Service (NRLS).

4.4 Selection of the Route

1] TLP provides the information about its address, uphill segment and dynamic failure information related to the upstream to the user. The address which matches the provider level routes of the user is given by the upstream.

2] The destination address of the sender is determined from the NRLS servers. The sender makes use of the Name-to-Route Lookup service (NRLS) to determine the segments of the route which leads to the destination. Hence information related to the downhill segment is obtained by the user.

3] Next based on the dynamic failure information and link level indicator agent, the sender selects the efficient path towards the destination. In Figure 1, let us assume that the path 3-4-V2-core-V8-13 is more secure as the probability of failure of this link is very less.

4] The sender node and the receiver node start exchanging the consequent packet, once the first packet reaches the receiver node. In case a failure is detected in the route by gateway feedback or timeout, then the user will take up another path by switching the addresses.

5 SIMULATION RESULTS

5.1 Simulation Setup

In order to test our protocol, the NS2 [10] is used. NS2 is a general-purpose simulation tool that provides discrete event simulation of user defined networks. We have used the ns-BGP extensions 2.0 for ns-2.33 for simulating the BGP architecture. The experimental setup is similar to Figure 2. In our simulation topology 10 AS nodes 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 2. CBR traffic is used with packet size 100 bytes. The traffic rate is varied from 1Mb to 5Mb. We consider AS8 as an attacker which performs prefix hijacking attack against the path AS9 to AS3.

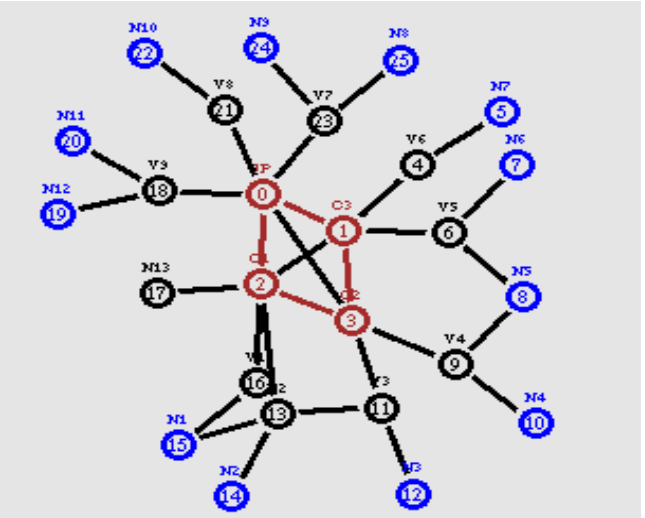

Fig. 2 Simulation topology

5.2 Simulation Results

In our first experiment, the packet sending rate is varied from 0.5Mb to 2.5 Mb. The packet loss ratio and throughput are measured. Figure 3 shows that packet loss ratio increases when the rate is increased. From the figure, we can see that the TARRP has very low packet loss ratio when compared to normal BGP scenario. In Figure 4, we can observe that, when the rate increases, the throughput also increases. From the figure, it can be seen that the throughput is high, when TARRP is applied.

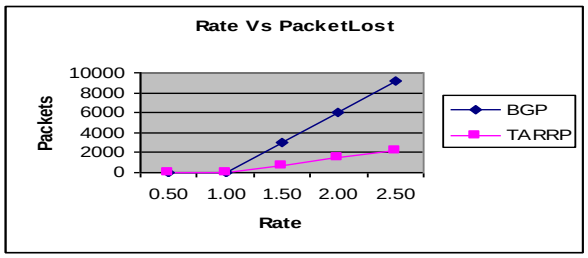

Fig 3: Rate Vs Packet Lost

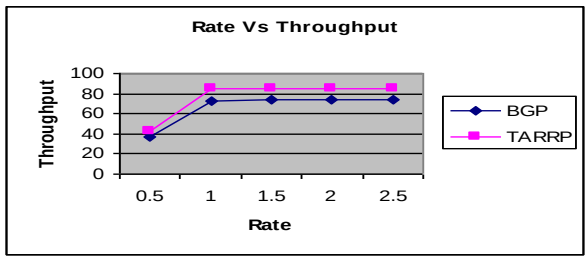

Fig 4: Rate Vs Throughput

In our second experiment, the performance is measured in various simulation intervals from 1 to 10 seconds. Figure 5 shows that packet loss ratio increases when the time is increased. From the figure, we can see that the TARRP has low Packet loss ratio when compared to normal BGP scenario. In Figure 6, we can observe that, at time 3 seconds, the throughput of BGP begin to degrade, as the attack is launched at 3 seconds. From the figure, it can be seen that the throughput is not affected, when TARRP is applied.

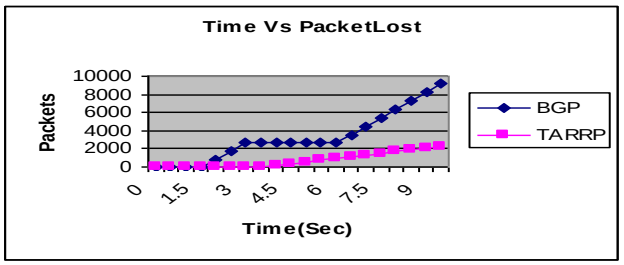

Fig 5: Time Vs Packet Lost

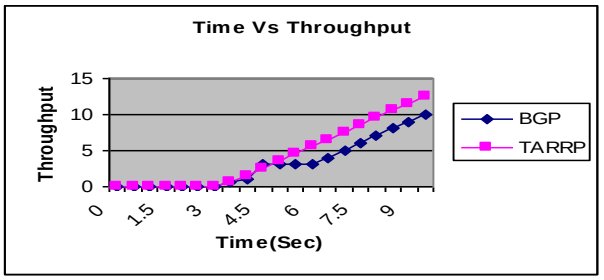

Fig 6: Time Vs Throughput

6 CONCLUSION

In this paper, we have developed a topology aware routing protocol for inter-domain routing in VPN which securely transfers the data. In this work before the transmission of the packet, the VPN gateway will register itself with the junction point, which allows the gateway to gain information about all the gateways that are connected to the core in the network. When a node wants to transmit a packet, the communication between the end users will take place in two phases. The first phase is the routing phase, in which the sender determines the upstream and the downstream using the topology learning protocol. The second phase is the authentication phase, where the VPN gateway authenticates the packet with the junction point and then transfers it towards the destination gateway after ensuring security of the packet. By simulation results, we have shown that our proposed protocol is better than the traditional routing protocols of VPN.

7 REFERENCES

[1] Alwin Thomas and George Kelley, "Cost-Effective VPN-Based Remote Network Connectivity Over the Internet", 2003.

[2] Seifedine Kadry and Wassim Hassan, "Design and Implementation of System and Network Security for an Enterprisse with Worldwide Branches", Journal of Theoretical and Applied Information Technology, ©2005 - 2008 JATIT..

[3] E. Ramaraj and S. Karthikeyan, "A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking", Journal of Computer Science 2 (9): 672-675, 2006, ISSN 1549-3636, © 2006 Science Publications.

[4] Christoforos Ntantogian and Christos Xenakis, "A Security Protocol for Mutual Authentication and Mobile VPN Deployment in B3G Networks", the 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07).

[5] Lookman Fazal, Sachin Ganu, Martin Kappes, A. S. Krishnakumar and P. Krishnan, "Tackling Security Vulnerabilities in VPN-based Wireless Deployments", 7 Jan 2008.

[6] Vassilis Prevelakis and Angelos Keromytis, "Designing an Embedded Firewall/VPN Gateway", this work was supported by DARPA under Contract F39502-99-1-0512-MOD P0001

[7] G. Malkin. Routing Information Protocol Version 2. RFC 2453, SRI Network Information Center, November 1998.

[8] J. Moy. OSPF Version 2. RFC 2328, Apr. 1998.

[9] R. Callon. Use of OSI IS-IS for Routing in TCP/IP and Dual Environments. RFC 195, Dec. 1990.

[10] Network Siimulator, http://www.isi.edu/nsnam/ns