Journal of Computer Science 10 (9): 1874-1880, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1874.1880 Published Online 10 (9) 2014 (http://www.thescipub.com/jcs.toc)

PERFORMANCE OF TOPOLOGY AWARE RELIABLE ROUTING PROTOCOL FOR LARGE SCALE VIRTUAL PRIVATE NETWORK

[1]Jayanthi Gokulakrishnan and [2]V. Thulasi Bai

[1]Sathyabama University, Chennai, India
[2]Prathyusha Institute of Technology and Management Chennai, India

Received 2014-02-20; Revised 2014-02-24; Accepted 2014-05-02

ABSTRACT

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). In VPN, the communication between the user ends 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. In this study, we propose a new reliable protocol called as Topology Aware Reliable Routing Protocol (TARRP) for large scale VPN and compare its performance with the traditional protocol, Boarder Gateway Protocol (BGP). In this protocol, the communication between the end to end nodes takes place in two phases: Routing phase and authentication phase. In the routing phase, the upstream and the downstream routing paths are determined by the source node using the topology learning protocol. Based on the dynamic failure information of links, the sender selects the failure-free path towards the destination. In the authentication phase, the VPN gateway authenticates the packet before it is transmitted through the core. Thus, this technique efficiently allows the packet to be transmitted with ensured security. By simulation results, we show that our proposed protocol is better than the traditional routing protocol of VPN.

Keywords: Routing Protocol, Authentication, Encryption, Throughput

1. INTRODUCTION

Enterprising organizations have various sites spread across different locations all over the world. These sites have to be interconnected for effective communication. But, having dedicated lines for communication involve lot of money and effort from the organizations. Hence, they prefer virtual private networks thereby the organizations reduce their costs. Thomas and Kelley (2003) have reported that VPNs are configured to be national or international private networks to its customer by the telecommunication carriers even when it shares its backbone trunks with additional customers. VPN is the major remedy to threats caused by the viruses and hackers as it maintains high security in the network lying between the companies and the users by authenticating and encrypting. In VPN, the communication between the two user ends 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. Kadry and Hassan (2008) have shown that 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. A Virtual

Corresponding Author: Jayanthi Gokulakrishnan, Sathyabama University, Chennai, India

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 corporate ventures. Mosharaf Kabir Chowdhury and Boutaba (2008) have stated that the VPN is an example for intranet which links all the sites of the large corporate ventures that are geographically dispersed.

The major problem in VPN network is related to connectivity that arises during the incorporation of the IPSec with NAT. This is due to the encryption of the IP address as well as the port number in IPSec. When the NAT device receives the encrypted IP and the port number, the decryption of this address cannot be supported by it. Hence the IP address cannot be transferred between the internal and the external networks. Another major problem faced in the VPN is auto fail over. If the network path in use fails, then ideally the network should route the traffic through some alternate link. But in VPN since the configuration is end to end, if any path fails then the new path has to be created separately to the live IP address. Another issue faced is the load balancing of VPN traffic over Multi-homed network. Yang and Gao (2006) have stated that since encryption and decryption is included in the VPN, additional computing power is needed as more number of factors has to be addressed. When compared with the public key cryptographic algorithms, RSA provides more security. Ramaraj and Karthikeyan (2006) have reported that the conversion of large amount of data is comparatively slow in RSA. Due to the variation in the response of the VPN to valid and the invalid username, vulnerabilities in the remote access VPN is high since the guessing of the valid username through dictionary attack is easy. In the authentication mechanism used, it is required that the wrong password/username login attempt must not give out any information as they entered data is wrong, as this will allow the attacker to easily determine if the entered username is valid or not. But this rule is not considered by most of the VPN implementation. The information carried in the VPN is very sensitive and the type of the network used is insecure and moreover full access to the internal network is provided by the remote access VPN, when IDS monitoring system cannot detect the VPN traffic. Hill (2005) has stated that VPN is prone to be a target to many attacks as security mechanisms is increasing in other fields like more organizations installing firewalls, moving Internet servers onto the DMZ and automatically patching servers. Jirapure and Jirapure (2013) have stated that Intrusion threat can be used against trusted VPN networks which effects on the data packets of the network, confidentiality and integrity of the packets.

2. RELATED WORK

The authors Ramaraj and Karthikeyan (2006) have 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. Ntantogian and Xenakis (2007) have 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 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 this method is that, its deployment may increase the computational overhead of the involved entities compared to the pure EAP-SIM.

Prevelakis and Keromytis (2007) have proposed 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. Its existence is transparent to the user, requiring no modification to the workstation configuration. To function in this role, Sieve has been designed to be compact, low-cost, requiring little administration or maintenance.

Ramadoss *et al*. (2014) have stated that the nodes periodically broadcast tree structure information to the best of its knowledge. A node can expand its scope of knowledge about the network based on the information it has been collected from its neighbours. Then this knowledge is exchanged among all the neighbouring nodes in the next iteration.

3. PROPOSED WORK

Most of the VPN suffer from security related and overhead problems. Malkin (1998) has stated that during the inter domain routing, the conventional RIP requires each gateway to resend its routing table periodically to all its neighbors thus increasing the delay in database updation where as in intra domain routing, the conventional OSPF and IS-IS protocol used requires built-in mechanisms to handle 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 study 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 reliably and in-order using the failure free secure shortest path. 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 is prone to attackers. 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 consists 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 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, 9 nodes and 9 VPN gateways. In this fig, node 3 sends the packet to node 9. The up graph at the source for the transmission of the packet consists of the uphill segment which can be 3-V2-core, 3-2-V1-core or 3-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-V9-9 or core-V8-9.

The transmission of the packet can be classified into two phases: The routing phase and the authentication phase. The initial phase is the topology aware routing phase where the encrypted packet from the node determines the upstream towards the core. Based on the dynamic failure information collected at the source along with the upstream information, the source node takes up the best uphill segment that leads to the core. Similarly at the destination end, the downstream information along with the dynamic failure information is collected and the best downhill segment is chosen by the source node. The second phase is the authentication phase which takes place as the packet enters the core. The VPN gateway in the uphill segment transmits the packet to the core only after authentication. The JP in the core provides the authentication to the packet transmission.

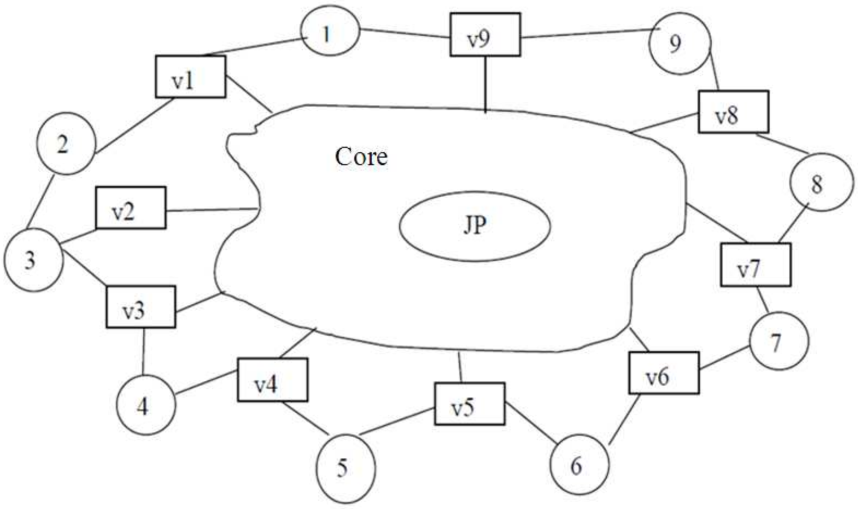

Fig. 1. Architecture of VPN

3.1. Forwarding

3.1.1. Outside the Core

The source node determines all the upstream node information towards the core for its packet transmission. The packet at the source node takes the path along the best failure free uphill segment using the dynamic failure information obtained along with the upstream information. Similarly at the destination end, the packet considers all the possible downstream nodes from the core and finally selects the best failure free downhill segment towards the destination node.

Initially every node uses the messages which it has heard from its neighbors and updates its topology database. The neighbor who is in the shortest failure free path is believed by the node and based on it the node determines the inconsistent messages from other neighbors. Since the messages transmitted along these nodes are in the required order, this results in the message transmission along the entire path to be in the accurate order and reliable. Hence the order of the message that is received from the neighbor which is on the shortest failure free path indicates the variations in the status of the message sequence in the link. Recursive computation of this path is possible. This is due to the fact that the particular node can determine if the node adjacent to it is a failure free node or not and similarly this new node can also determine the nature of its adjacent neighbors. In this way, the particular node can establish an overall path that is failure free up to any length in the network.

3.1.2. Within the Core

The steps involved in the transmission of the packet are given in the algorithm as follows:

Algorithm:

1] Initially the gateway at the source sends a route request, R to JP.

2] The JP responds by submitting the route response, R to the gateway if the gateway is already registered in that JP.

3] The gateway then requests authentication ticket for the source node from the JP.

4] The JP responds by providing the requested authentication ticket, using the pair wise shared key for encryption.

5] The gateway now directly contacts the service providing gateway i.e., the gateway at the destination and requests an authenticator.

6] The destination gateway responds ensuring secure interaction.

A private and mutually authenticated channel is used for the transfer of messages (1) and (2). In the first two steps, privacy and trust are of higher priority in order to avoid the JP from revealing the information about the other gateways that are online. An important feature of message (2) is it allows the JP to select access control measure by disclosing only a part of the information of the R to some particular gateways. This feature is advantageous as it permits the JP to separate the nodes under the control of a single gateway logically on the basis of the traffic disclosure levels and also permits the nodes to take control over the connectivity degree whenever it is being controlled by the network resources. Once the route response R is obtained by the gateway at the source requesting the communication, after the transfer of message (2), the source gateway can request the authentication tickets to its members. In the case the communication has to be developed between all the members of the gateway, then for every node, the gateway requests the JP for the communication credentials. As seen in message (4) and (5), the credentials will be distributed to the nodes and then it is verified accordingly. Hence forth, the trust is maintained between the two involved gateways and hence as seen in message (6) starts with route advertisement. This is then repeated from message 3 to message 6 for every peer. Now the source gateway and the destination gateway encrypt the traffic before transmission by sharing the pair wise session key, Kc,s.

4. SIMULATION RESULTS

4.1. Simulation Setup

The experimental evaluation of the proposed algorithm is performed using Network Simulator NS2. NS-BGP extension 2.0 in NS -2.33 is used for simulating the BGP architecture. The experimental setup is shown in the **Fig. 2**.

The simulation topology is described as follows: 10 Autonomous Systems (AS) nodes are connected with a central core. Each AS is provided with a network addresses from 10.0.0.1 to 10.0.9.1. The link bandwidth is set to be 10Mb and link delay is assumed to be 20 ms. BGP agent is attached to each AS connected with neighbor AS as shown in the **Fig. 2**. CBR traffic is set to be 100 bytes. The variation of traffic rate is from 1Mb to 5Mb. The node AS8 is considered as an attacker which performs prefix hijacking attack against the path AS9 to AS3.

Figure 3 and 4 show the throughput for attack and no-attack scenarios for both TARRP and BGP at increased packet sending rates. It can be seen that, while TARRP has 37% of throughput degradation in presence of attackers, BGP has 45% of throughput degradation, which is 8% higher than TARRP.

Figure 5 and 6 show the throughput for attack and no-attack scenarios for both TARRP and BGP, at increased time intervals. It can be seen that, while TARRP has 40% of throughput degradation during attack, BGP has 47% of throughput degradation, which is 7% higher than TARRP.

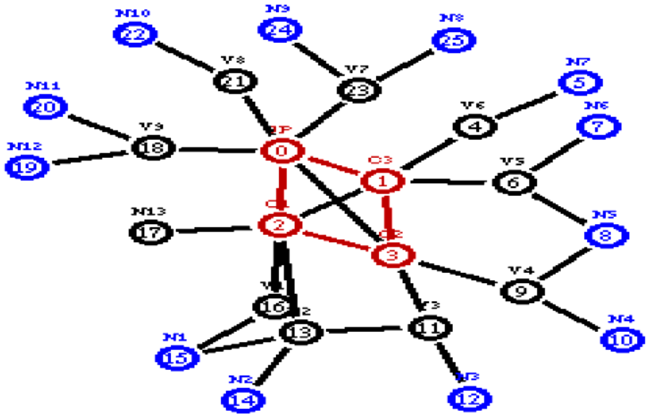

Fig. 2. Simulation topology

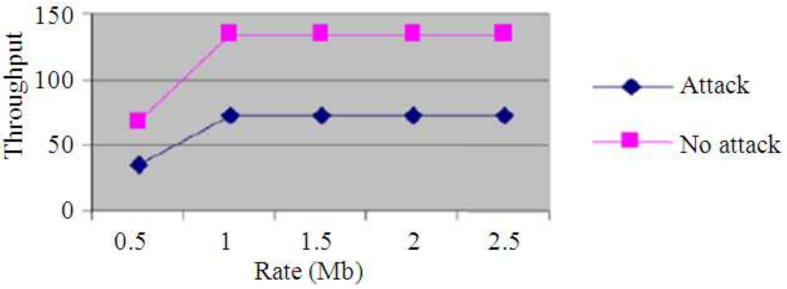

Fig. 3. Rate Vs. throughput (BGP)

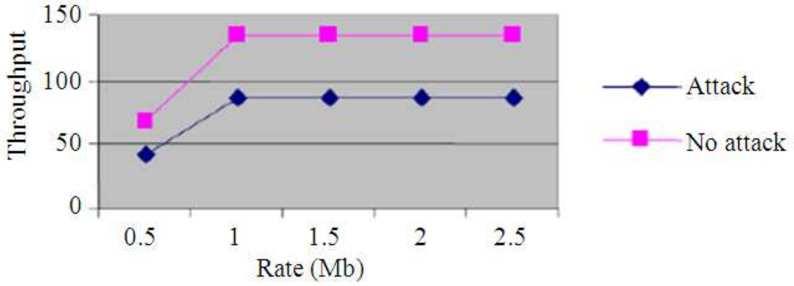

Fig. 4. Rate Vs. throughput (TARRP)

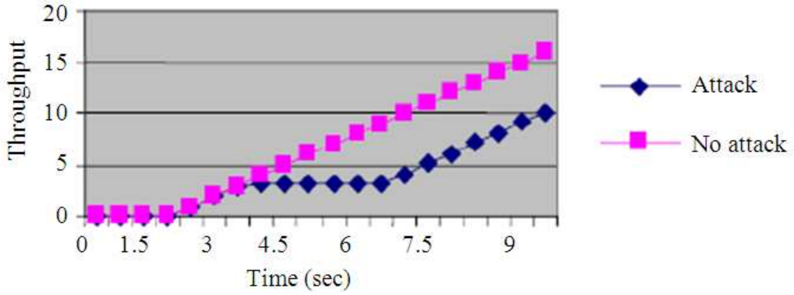

Fig. 5. Time Vs. throughput (BGP)

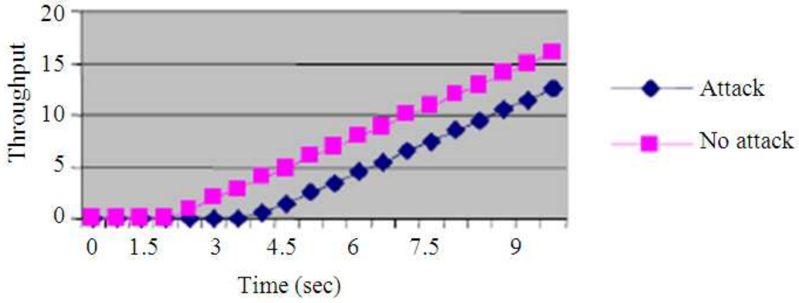

Fig. 6. Time Vs. throughput (TARRP)

5. DISCUSSION

The parameters taken for study are Rate vs. Throughput and Time vs. Throughput. Since throughput determines the successful data transfer in a network, this attribute is taken as the main study. . In this experiment, the results of attack scenario with normal non-attacking scenario for both BGP and TARRP are compared. Throughput degradation is very minimal in the proposed method when compared to the traditional method, BGP. Using the same setup, the latency and the bandwidth of the network can be analyzed in the future study.

6. CONCLUSION

In this study, a topology aware reliable routing protocol for inter-domain routing in large scale VPN is proposed and its performance is compared with the traditional protocol BGP using network simulator NS2. It is seen from the results that the new protocol (TARRP) performs better in terms of throughput in the event of attack or no-attack scenarios. 10 AS nodes are considered in the simulation setup. In the future work, the number of As nodes can be increased and the performance of the new protocol can be checked for its consistency. We can also take some other quality attributes for evaluating the performance of the new protocol.

7. REFERENCES

Hill, R., 2005. Common VPN security flaws. NTA Monitor Ltd.

Jirapure, R. and S. Jirapure, 2013. A critical review of security mechanisms in virtual private networks. Int. J. Scientific Eng. Technol., 2: 1168-1172.

Kadry, S. and W. Hassan, 2008. Design and implementation of system and network security for an enterprise with worldwide branches. J. Theoretical Applied Inform. Technol., 4: 111-118.

Malkin, G., 1998. RIP Version 2. RFC 2453, SRI Network Information Center.

Mosharaf Kabir Chowdhury, N.M. and R. Boutaba, 2008. A survey of network virtualization. University of Waterloo.

Ntantogian, C. and C. Xenakis, 2007. A security protocol for mutual authentication and mobile VPN deployment in b3g networks. Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Sept. 3-7, IEEE Xplore Press, Athens, pp: 1-5. DOI: 10.1109/PIMRC.2007.4394363

Prevelakis, V. and A. Keromytis, 2007. Designing an embedded firewall/VPN gateway. Drexel University.

Ramadoss, P., S.M. Yakub and S. Annaji, 2014. A preemptive link state spanning tree source routing protocol for mobile adhoc networks. J. Comput. Sci., 10: 85-90. DOI: 10.3844/jcssp.2014.85.90

Ramaraj, E. and S. Karthikeyan, 2006. A new type of network security protocol using hybrid encryption in virtual private networking. J. Comput. Sci., 2: 672-675. DOI:10.3844/jcssp.2006.672.675

Thomas, A. and G. Kelley, 2003. Cost-effective VPN-based remote network connectivity over the internet.

Yang, B. and T. Gao, 2006. Building a secure and reliable network via multi-homed VPN. Proceedings of the IJME-INTERTECH Conference, (INTERTECH’ 06).