Al-Rafidain Engineering Vol.13 No.4 2005

Analysis and Design of a Novell VPN Switch

Dr. A.I.A.Jabbar
University of Mosul
College of Engineering
Electrical Eng. Dept.

Ahmed Badir Mahmood
Directorate of Electrical
Transmission Projects
Communication Dept.

Abstract

Security problems take an important part of computer network study in which several techniques were developed for this purpose. Virtual Private Networks (VPNs) are considered as an active form for providing secure networks. The key feature of VPNs is that they are able to use public networks like the Internet rather than rely on expensive private lines.

The aim of this paper is to design a VPN switch with the help of simulink software provided by MATLAB 6.5. The VPN switch is a single hardware device, it has the ability to support firewall, encryption, authentication, and data integrity for secure tunneling across managed IP networks and Internet.

Introducing scrambling code within a VPN switch for encryption is something new. The basic advantage of this method is to eliminate long headers, which are usually dedicated for authentication and encapsulation in IPSec. Therefore an increase in the bandwidth efficiency of the channel is expected. Larger values of spreading factor show better probability of error and data integrity in spite of the decrement in the bandwidth of the channel in some cases.

[illegible]

Submitted 24 th August 2004 Accepted 11th April 2005

www.manaraa.com

1.Introduction

Dnd for computer communication networks which is supported by the huge development of computers from the size and economize points of view, new approaches and techniques have been produced such that people can share expensive resources economically [1]. At the beginning, security did not get a lot of attention, but now millions of people are using networks for private things (for example banking). Therefore network security become a potentially massive problem [2 .[In general there are four categories of network attack:
Interruption is an attack on availability, for example logic bomb, viruses or worms.
Interception is an attack on confidentially, like wiretapping to capture data passing through a network.
Modification is an attack on integrity, for example modifying the content of messages being transmitted in a network.
Fabrication is an attack on authenticity. Like insertion of spurious messages in a network

One of the solutions for these problems is possible by using a secure network known as virtual private network (VPN .(The technical term virtual is used because VPN is not a physically distinct network, the term private means that communications is limited among certain number of devices and the term network means any number of devices that can communicate together using different types of protocols [3].

VPNs have merged the advantages of public and private networks. It allows a company to have a private network by using a public network as a communication media.
It is also important to mention that VPN can be considered as the evolution of wide area networking (a private network constructed within a public network infrastructure such as the global Internet at a great saving in cost).
The famous security protocol being used in the conventional VPN is known as IPSec [4]. It is classified as transport and tunneled modes. Transport mode of IPSec can be used only when end-to-end security is desired, while in tunnel mode is normally used when the ultimate destination of the packets is different from the security termination point.

IPSec protocols currently applied in the design of a VPN are [5:[
AH (Authentication Header) in transport mode, AH in tunnel mode, ESP (Encapsulating Security Payload) in transport mode and ESP in tunnel mode. In practice, AH in tunnel mode is not used because it protects the same data that AH in transport mode protects. Therefore IPSec can apply either AH, ESP or both headers (ESP- AH) in the design of a VPN.

AH provides a proof of the correctness of the received packets (data integrity, and anti replay protection), but it does not provide confidentiality. It is simply a header and not a header plus trailer. AH does not encrypt any portion of the protected IP datagram. AH is just used to guarantee that the received packet was not modified in transit.

ESP provides all that AH provides in addition to the optional data and limited traffic flow confidential. But the scope of coverage of authentication in AH is better than that of the ESP. The length of AH header is 12 bytes while the length of ESP header is 20 bytes or more .

المنارة للاستشارات
www.manaraa.com

When both AH and ESP are used, ESP should be applied first. The reason is obvious. If the packet is first protected using AH then ESP, the data integrity is applicable only for the payload. This is not desirable because the data integrity should be calculated over as much as possible. If the packet is protected using AH after it is protected using ESP, then the data integrity applies to the ESP payload that contains the payload.

Figure 1 shows the packet format with AH and ESP.

1. Theory of VPN

The foundation of virtual private networks is based on encryption and encapsulation types of security techniques. They can be combined in different implementation topologies.

Encryption is defined as the process of protecting information from unauthorized viewing or use, especially during transmission or when it is stored on a medium [6]. The two types of encryption are:

**Symmetric* cryptography tends to be much faster to deploy, and is commonly used to exchange large packets of data between two parties who know each other. They use the same private key to access the data sources.

**Asymmetric* systems are far more complex and require a pair of mathematically related keys - one public and one private - in order to be accessed. This method is often used for small and more sensitive packets of data or during the authentication process.

Encapsulation is defined as the process of hiding information about an object, such as internal data structures and code from intruders. It can be achieved by isolating the internal complexity of an object's operation from the rest of the application.

User authentication is an important property of VPN connections; (for example users using client/server mode of communication must be authenticated by each other as a matter of protection against unauthorized users).

Data authentication and integrity are very important as far as security is concerned. They ensure that the data being sent on the VPN connection is originated at the destination is not modified during transmission. This can be achieved by applying a pre-agreement cryptographic checksum between the two users based on an encryption key within the data [7].

Virtual private networks can be created at the transport, network and data link layers of the TCP/IP model [3], as follows :

Encryption technique is the most prevalent method of providing virtualization at the application layer, e–mail is an example of this kind of network.

It is important to mention that the TCP/IP model provides two protocols at the transport layer, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). The choice of using TCP or UDP is entirely up to the application. This layer identifies the source and destination ports. UDP is used for fast and

المنارة للاستشارات
www.manaraa.com

simple messages. Encryption and other security services such as authentication, integrity, and confidentiality can implement VPN at the transport layer.

The network layer is responsible for routing packets through out a network such that reliable communication can be achieved. According to TCP/IP model, the available network protocols are IPv4 and IPv6. The first one (Internet Protocol version 4) is the most prevalent network protocol. It uses simple addressing scheme and provides connectionless service. Network layer VPN could be created using controlled route leaking, tunneling, and network layer encryption methods as follows:

Controlled Route Leaking. According to this method only certain networks receive routs for other networks which are within their own community of interest.

Tunneling is the process of sending packets to a computer on a private network by routing them over some other network, such as the Internet. The other network's routers cannot access computers on the private network. Both the VPN client and server use tunneling to route packets securely to a computer on the private network by using routers that know only the address of the private network server.

Sending specific portions of network traffic across a tunnel is another method of constructing VPNs. The most common tunneling mechanisms are GRE (Generic Routing Encapsulation (tunneling between a source and destination router, router-to-router or host-to-host tunneling protocols such as PPTP (Point-to-Point Tunneling Protocol (tunnels.

Network Layer Encryption. Encryption technologies are extremely effective in providing the segmentation and virtualization required for VPN connectivity, and can be deployed at almost any layer of the protocol stack.

Finally, the data link layer, which is responsible for packet transmission on the physical media, can also be used to create VPN. Examples of data link layer protocols are HDLC, and ATM (Asynchronous Transfer Mode). It uses hardware devices for encryption and this method provides higher speed in comparison with the other methods.

2. The Proposed VPN Switch

VPNs can be created using either pure software algorithm or hardware techniques. Software VPN is easier to be implemented but not very efficient, this is due to the fact that software encryption algorithms are less secure and slower than hardware encryption algorithms. The latter requires a device (switch) which connects the VPN users (usually LAN) with the Internet.

Conventional VPN switch is simply a single hardware device [8], it provides services such as: firewall, encryption, authentication and data integrity for secure tunneling across managed IP networks and the Internet. This switch consists of CPU, RAM, ROM, Interface circuits and the operation software (it is always written in assembly language). Figure 2 shows a conventional VPN switch block diagram.

المنارة للاستشارات
www.manaraa.com

In this research, a new technique for a VPN switch encryption is introduced. It is based on the theory of scrambling code, which randomizes the output data of the switch in a known manner. Accordingly, the VPN switch resultant data appears to be hard for any one to break it. Golden scrambling code type is suggested. It is very useful because of the large number of codes that can be provided by its generators [9]. Practically, they are generated by module–2 addition of a pair of maximal equal length code sequences. They are added chip by chip with synchronous clocking (The change in state from zero to one or from one to zero is called chip). Figure (3) shows the circuit diagram of a simple scrambling code generator. It is worth while to mention that a generator having n registers can generate length sequence equal to ($2^n - 1$.(

The scrambling code appears to provide a strong level of encryption as follows:
If the spreading factor (SF = chip rate / bit rate) is equal to one, (the period of the chip is equal to the period of the bit) then multiplying data bits with the chips sequences, will produce a new sequence completely different from the input data. In the receiver of a VPN switch, an identical Golden sequence is to be generated; this sequence is multiplied with the received sequence to recover the original data (descrambling).

Higher level of security is possible if larger values of spreading factor are to be used. This means that different chip and bit period values are exist now (chip rate is twice bit rate). Depending on the SF value, every bit will be replaced by few chips. An improvement in the probability of error and in data integrity is possible if we use spreading factor greater than one (for example 2 or 3), this is true because every bit is splitted into two or more chips, so if the value of one chip is changed by noise or any other effect it may have still the possibility of recovering the original data successively.

On the other hand, increasing the magnitude of the spreading factor will cause complicated matching problem at the receiver part of the VPN switch. This problem can be solved into hardware by controlling the frequency of the encrypted data clock depending on the spreading factor value. In other words, the time (clock) of moving data from a processor unit to the output port becomes a function of the spreading factor value.

Although this technique is not compatible with the present systems and networks, it is still suitable for some special applications like the one shown in figure (4).

An alternative software solution is also possible, as follows:

If the SF=2 Ûthen the data bit rate must be reduced softwarely to half its original rate; therefore, the doubled duration bit (each bit duration is doubled) before scrambling can accommodate two chips (i.e. each chip width = the original bit width). According to this technique, the clock rate is kept constant, but the packet length will be doubled and a significant overall delay is expected. This method is compatible with the existing networks and can be connected to the Internet.

A VPN switch has a unit which is devoted for the authentication process (*option*) between VPN switches; the suggested type is based on the *message*

المنارة للاستشارات
www.manaraa.com

encryption method (closed key). Figure (5) shows an example of the authentication between two VPN switches.

The VPN switch contains a unit, which is devoted to add (encapsulate) the address of the destination switch to the scrambled packet. The resultant frame will be directed to a user within the lookup table of the destination switch.

The VPN switch contains also important units for encapsulation and de-encapsulation processes. Figure (6) shows a block diagram for the de-encapsulator circuit, using Simulink of MATLAB 6.5.

The scrambled VPN switch contains an address checking unit which is considered as a packet filter; it checks source and destination IP addresses and ports numbers, if they belong to a VPN member, then the packet will be accepted, otherwise the packet will be rejected. Figure (7) shows a block diagram of the address-checking unit. Each block contains some logic gates arranged in a specified way.

The generated packet from this switch does not require any additional headers like that of the IPSec techniques, therefore an increase in the throughput of the channel is expected.

Finally, the VPN switch contains some buffers that are required to store packets during the different processing times. Figure (ē) shows a block diagram of the proposed VPN switch (hardware type .(

3. Simulation study

This study deals with the simulation of a VPN LAN that consists of two VPN switches and two Ethernets interconnected together, (see Figure 4).
The simulation is based on MATLAB version (6.5) with the following assumptions:

1. User Datagram Protocol (UDP) is selected as the transport layer (TCP/IP model). UDP is preferred when someone wants to establish his own protocol.
2. The Internet Protocol version 4 (IPv4) is the protocol being used by the switch.
3. In case of software technique and for more security, the following is applied. If the data frame length is more than 750 byte/frame, then the frame is considered as a long frame and the switch uses spreading factor (SF) =1. When the length is less than 750 byte/frame, the frame is considered as short frame and the switch uses SF=2 or greater.
4. Maximum packet size within the Ethernet LANs is 1518 bytes (maximum payload of data 1480 bytes + 20 bytes for IP header + 14 bytes for Ethernet layer header + 4 bytes of CRC used for detecting errors). This is considered as a long frame, the short frame length is less than half the length of the long frame.
5. Different scrambling codes can be used in a sequence known to both source and destination switches.
6. The header must contain few bits that are used to inform other VPN switches that the packet being received is of the scrambled type and the magnitude of the SF.
7. The channel bandwidth is greater than the scrambled packet bandwidth.

المنارة للاستشارات
www.manaraa.com

A VPN switch will apply the following algorithm in the case of transmitting packets to the other switch for the network shown in Figure (4).

1. Examining the IP destination address, if it is not in the list of the VPN LAN, then the data will be sent without scrambling and the switch will behave as a bypass element (repeater). When IP destination address appears to be one of the VPN members (look up table) and belong to the other switch, the source switch will attach the address of the other switch.
2. Scrambling the IP datagram (it refers to the payload plus users IP addresses).
3. Encapsulating the scrambled datagram with the unscrambled IPv4 headers (source and destination switch's addresses).
4. In case of using spreading factor equal to n, the clock rate of the switch must be multiplied by n. This is important to equalize the change in the output rate.
5. Changing the voltage of the data baseband from unipolar to bipolar before transmission in order to reduce the noise effect of the channel and improve the decision process at the receiver.

The receiver of the switch applies the following algorithm

1. The voltage level of the received signal is changed back from bipolar to unipolar.
2. De-encapsulating the scrambled packet, then checking IP addresses and port numbers of the source and destination switches.
3. Descramble the original packet to extract the address of the intended user, after that, the unscrambled packet will be directed to it.
4. Finding the spreading factor value in order to use the right encryption method and the suitable clock rate.

As mentioned before, IPSec protocols requires large headers to accommodate the necessary information being used in the creation of a given VPN, therefore, and as far as the efficiency is concerned, the hardware scrambled technique is expected to provide a better efficiency than other IPSec protocols. But this is not the case with software scrambling technique (for SF > 1) except for short length packets where the efficiency may approach IPSec efficiency.

Figure (9 (shows the efficiency of the proposed switch and other IPSec protocols as a function of the packet length. It is calculated using the following formula:

$$\xi = \frac{DataLength}{FrameLength} \quad \ldots 4.1$$

Finally the effect of the VPN switch on the Ethernet user can be modeled as follows:

The VPN switch whether it is connected with a linear or hub Ethernet LAN configurations will behave like any other user in the network, therefore, the throughput of any local Ethernet LAN with a VPN switch is identical to the traditional single Ethernet LAN. This result is related to the fact that the VPN switches will isolate the different Ethernet LAN from each other.

Figure (10) shows the relationship between the throughput and the offered load. It is identical with the figure (4.7) shown in reference [10].

المنارة للاستشارات
www.manaraa.com

5.Conclusion

VPNs have emerged the advantages of public and private networks. It is a secure and an economic network. It can be implemented at any layer of the TCP/IP protocol stack, either by software or hardware devices (Switches).

Introducing scrambling code as a proposed method of generating VPNs proved to be an efficient technique and an improvement in the utilization of the channel is obtained due to the shorter headers being used as compared with other techniques.

It is obvious that introducing scrambling codes will increase the security performance if it applied to the conventional IPSec protocols.

www.manaraa.com

References

1. Douglas E. Comer " ûComputer Networks and Internets û" Prentice Hall Incď ûrd edition, 2001.

2. William Stallings " ûCryptography and Network Security û" Prentice Hall Inc, 1999.

3. Paul Ferguson, and Geoff Huston û" What is a VPN ? ",2004. http://www.nanog.org/mtg-9806/ppt/ferguson

4. David Leon Clark " ûIT Manager's Guide to Virtual Private Networks ", Mc–Graw Hill Publishing, 1999.

5. Naganand Doraswamy, and Dan Harkins " ûIPSec û" Prentice Hall Inc., 1999.

6. Find VPN û"What Is VPN Encryption?", 2003 http://www.findvpn.com/articles/encryption.php

7. Bradley Dunsmore, Jeffrey W. Brown, and Michael Cross û"Internet Security", Syngress Publishing, 2001.

8. Nortel. Contivity VPN switches čċċČ . http://www.nortelnetworks.com/products/01/contivity/techspec.html.

9. Robert C. Dixon " ûSpread Spectrum Systems û" John Wiley & Sons Inc., 1984.

10. Qutaiba I. Ali û"Studying Local Area Networks Using Simulation Technique", M.Sc. Thesis, University of Mosul, 1998.

المنارة للاستشارات
www.manaraa.com

New IP Hdr	**Orig IP Hdr**	**TCP Hdr**	**Data**

(a) Proposed Frame Format Using Scrambling Technique

New IP Hdr	**AH**	Orig IP Hdr	**TCP Hdr**	**Data**

(b) Authentication Header of IPSec (AH)

New IP Hdr	ESP	**Orig IP Hdr**	TCP Hdr	Data	ESP Trlr	ESP Auth

(c) Encapsulating Security Payload of IPSec (ESP)

New IP Hdr	ESP	IP Hdr	AH	Orig IP Hdr	TCP Hdr	Data	Esp Trlr	ESP Auth

(d) Frame Format with ESP and AH

Figure 1 Frames Format

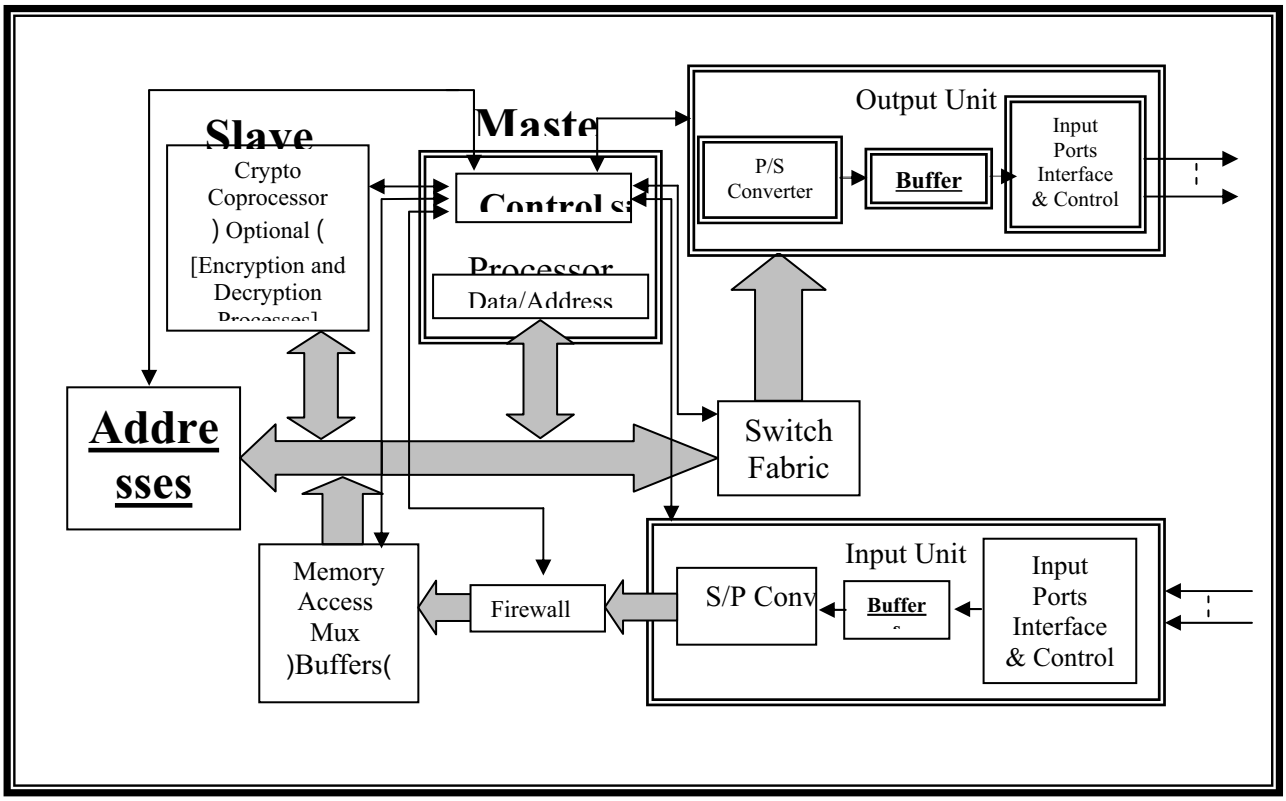


Figure 2 Block Diagram of a Conventional VPN

www.manaraa.com

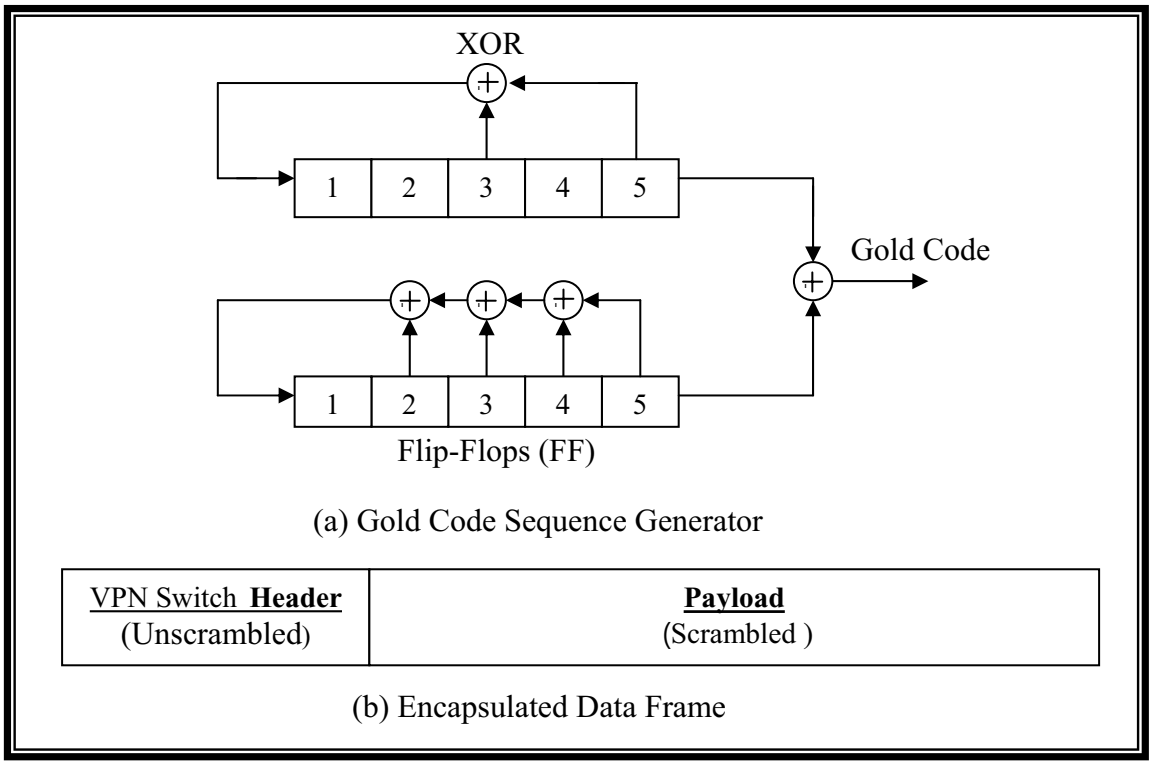


Figure 3 Gold Code Sequence Generator with the Data Frame

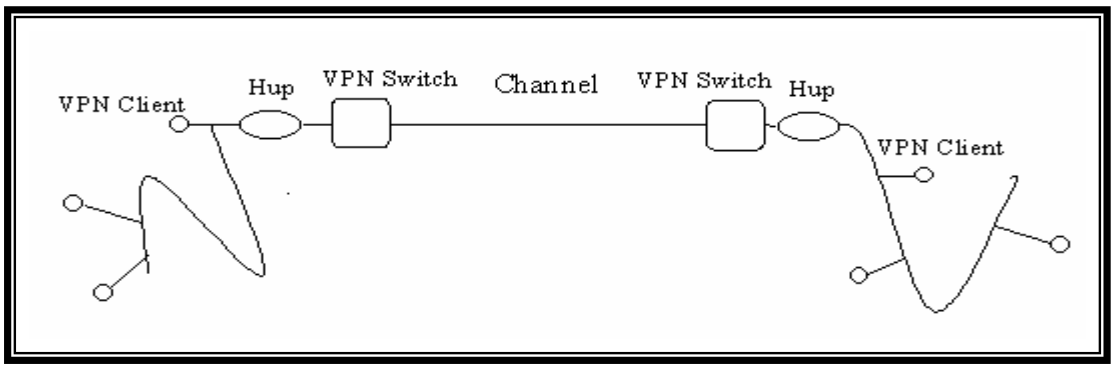


Figure 4 Special LAN using Scrambling as Encryption Method

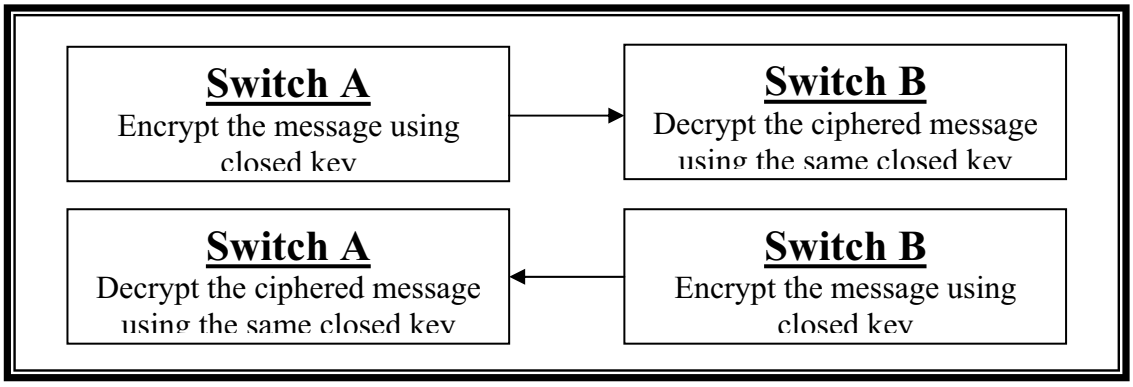


Figure 5 Simple Example of Authentication Process Between Two VPN Switches

www.manaraa.com

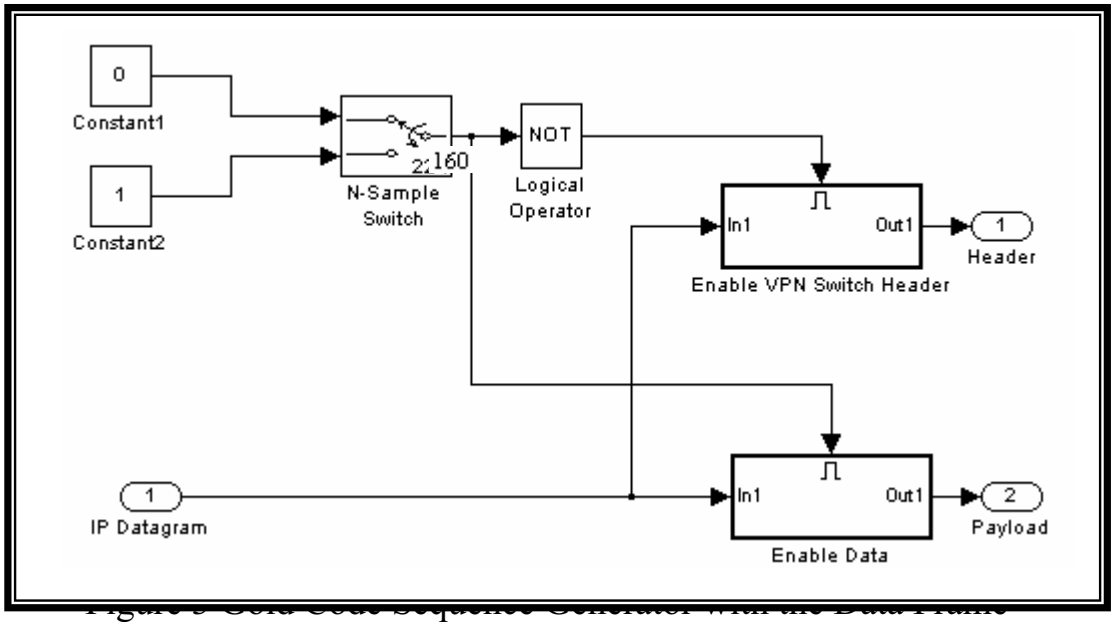


Figure 6 VPN Switch De-encapsulation Unit

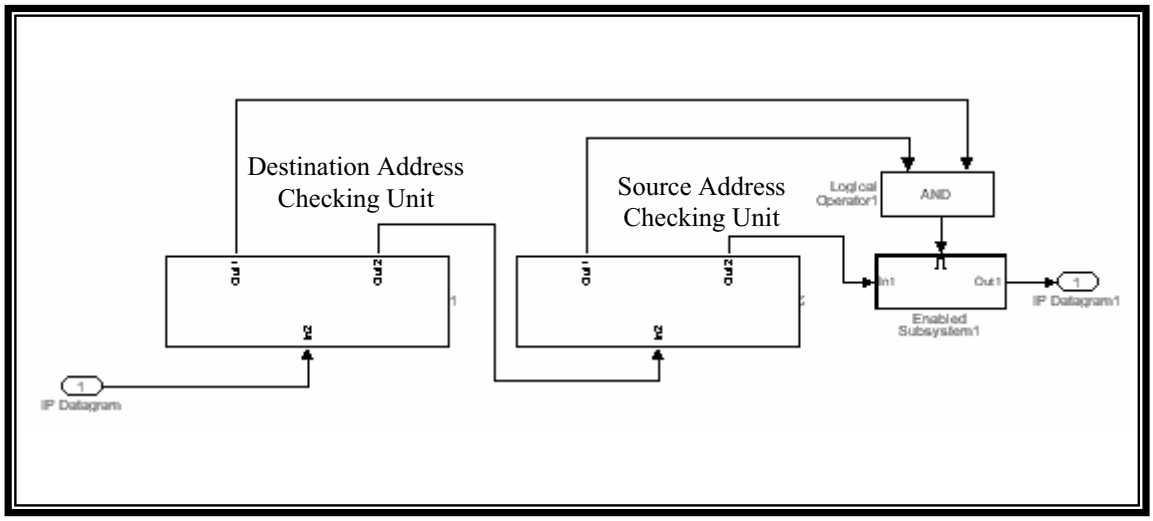
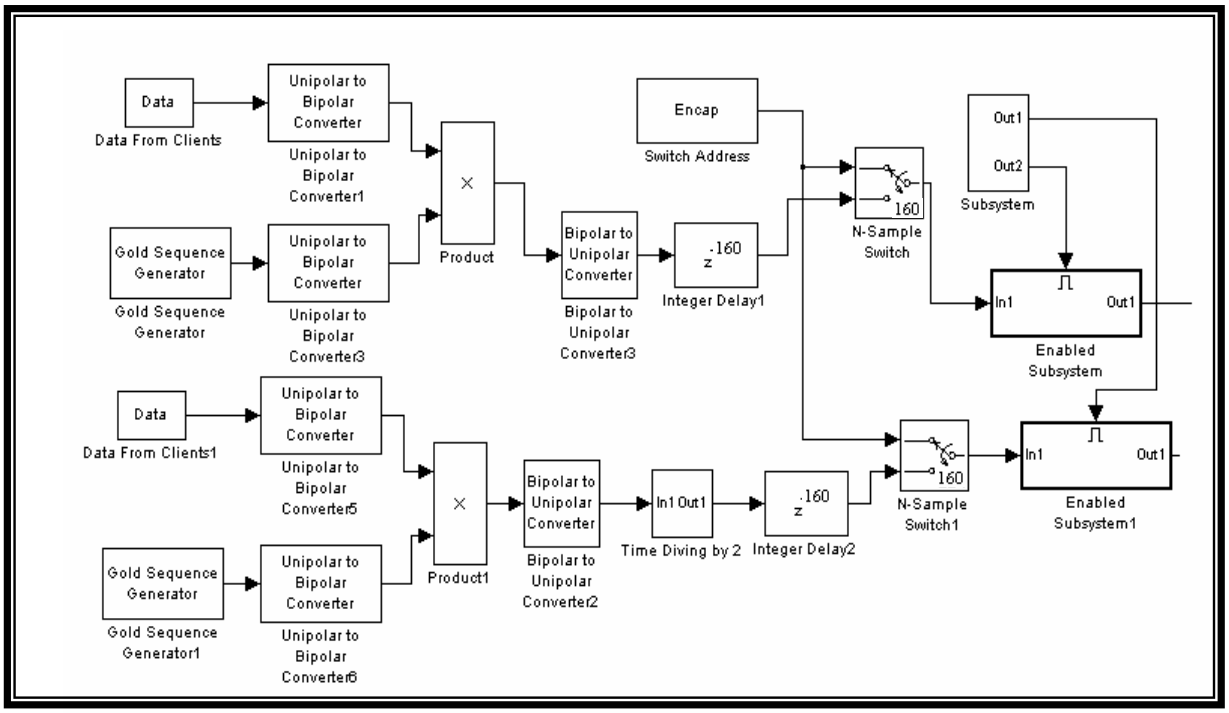
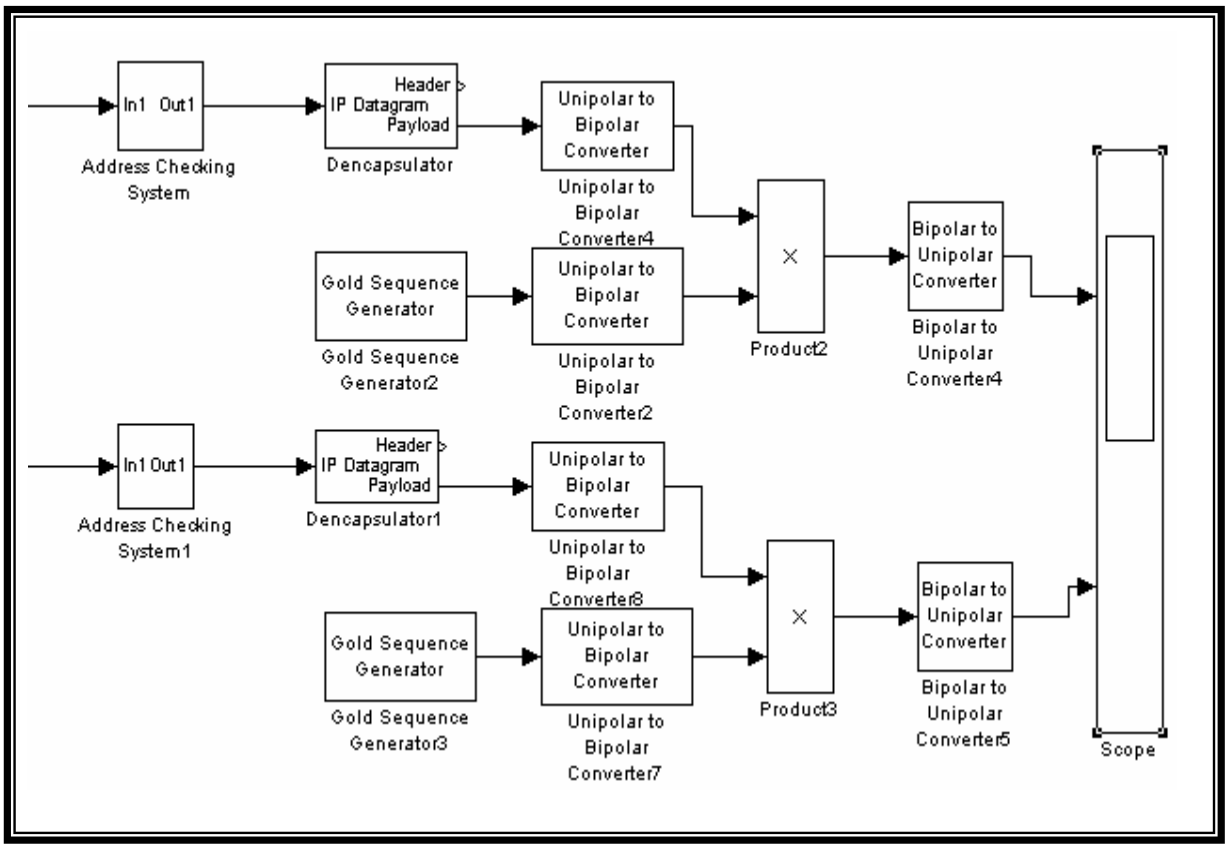


Figure 7 Source/Destination Address Checking Unit

www.manaraa.com



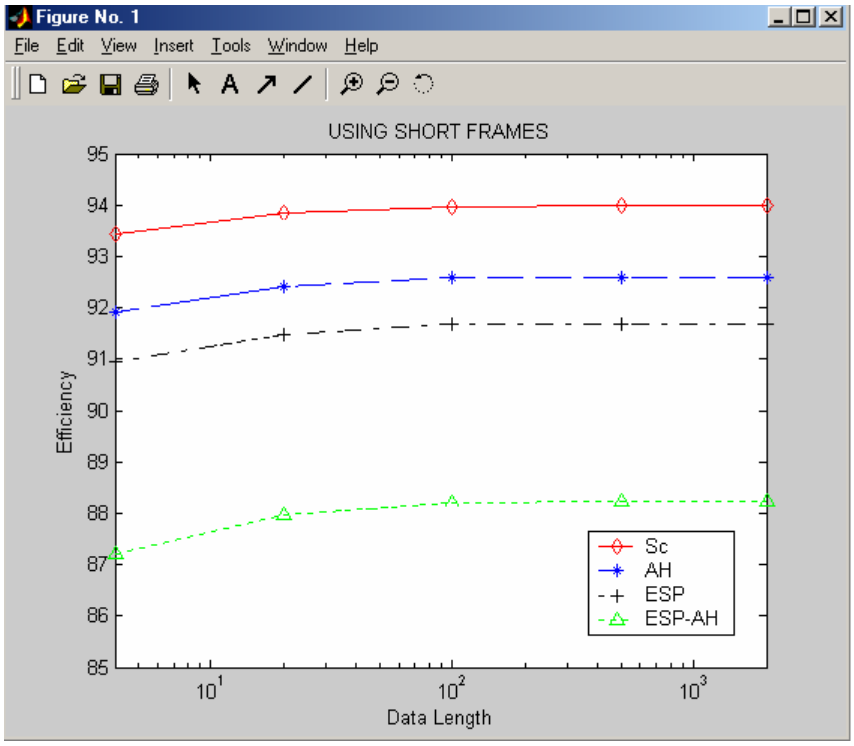
(a) Transmitter Unit



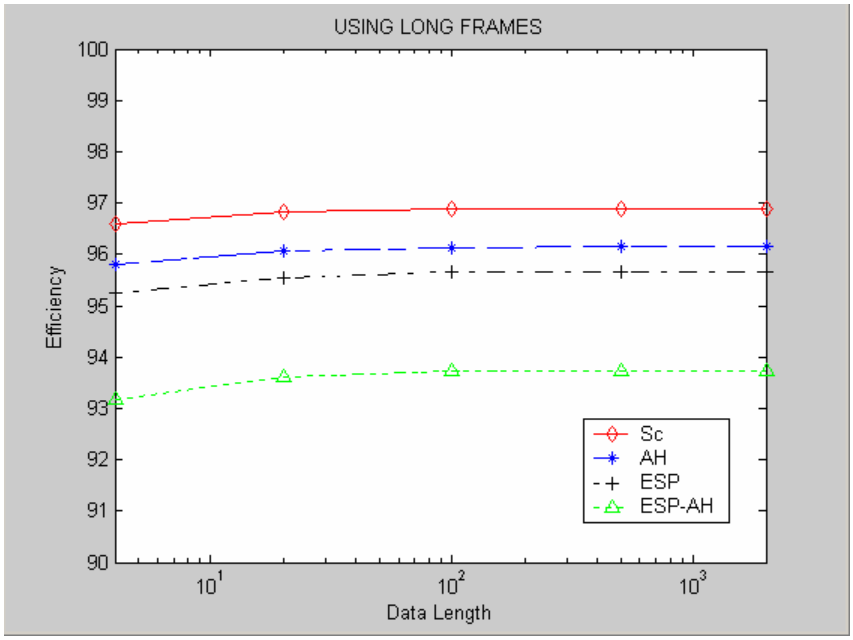
(b) Receiver Unit

Figure 8 Block Diagram of The Proposed VPN Switch

www.manaraa.com



(a) Efficiency of The Switch Using Short Frames



(b) Efficiency of The Switch Using Long Frames

Figure 9 Efficiency of The Switch

www.manaraa.com

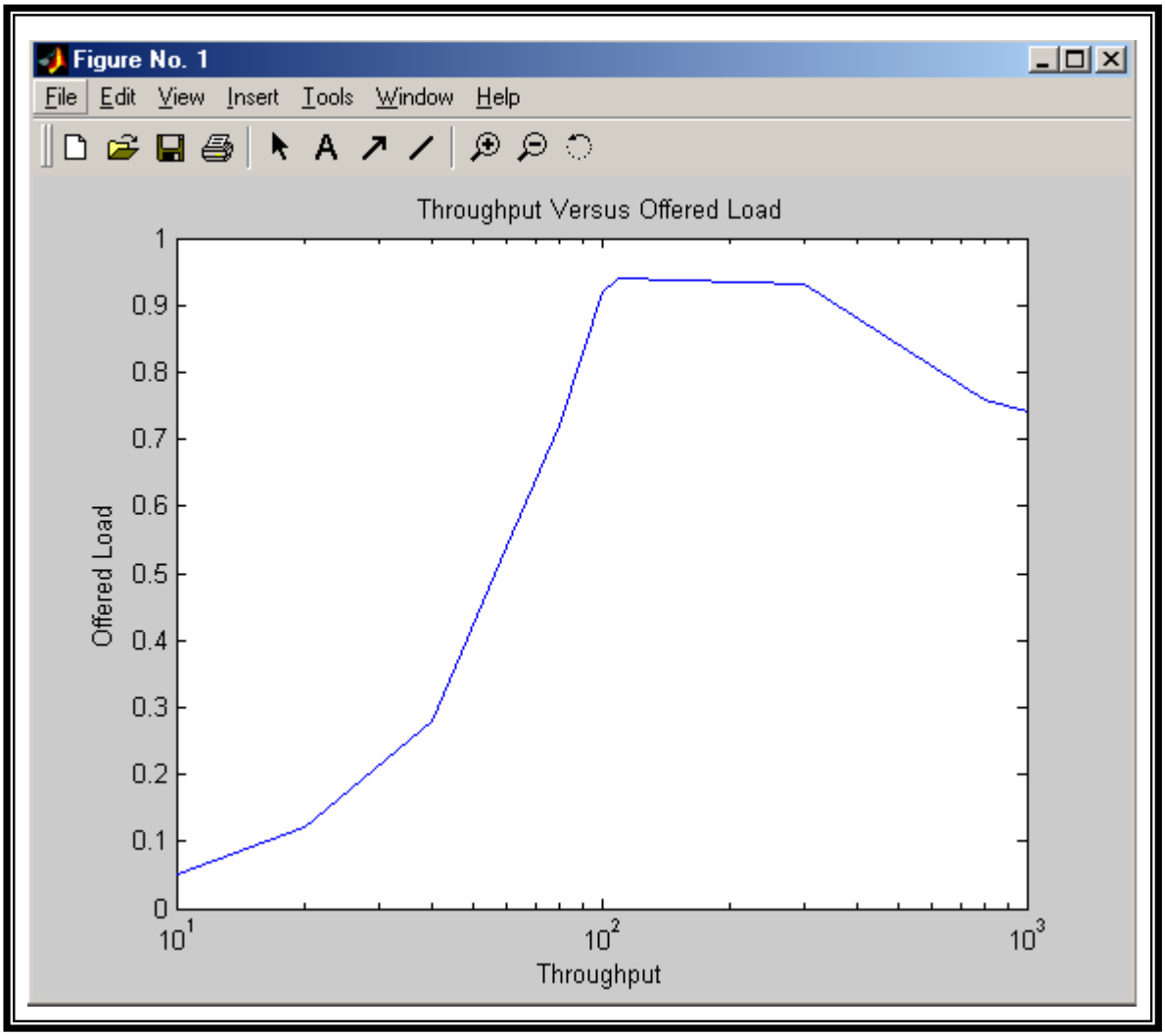


Figure 10 Relationship Between The Throughput and

www.manaraa.com