IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 1, Ver. II (Jan – Feb. 2015), PP 85-91
www.iosrjournals.org

The effect of Encryption algorithms Delay on TCP Traffic over data networks

Esam Suliman Mustafa Ahmed[1], Dr.Amin Babiker A/Nabi Mustafa[2]
[1, 2]*(Faculty of Engineering / AL-Neelain University, Sudan)*

Abstract: Security is a big concern for data networks users. Data encryption considered to be one of the best solutions for security issues. There are some standard encryption algorithms that used to encrypt transferred data using encryption keys. DES, 3DES, and AES are common encryption algorithms used in TCP/IP networks. Virtual Private Networking (VPN) is the one of the best security mechanisms that used encrypted virtual tunnels .In this paper the effect of encryption delay on TCP based applications is discussed. Simulation is a major part of this Paper. Increasing the encryption delay and then comparing the effect of that delay on TCP protocol through different scenarios is the methodology of the study, using OPNET. One server supporting HTTP and DB services is used. Four scenarios have been simulated. Results were compared by measuring the effect of applying different encryption delay values to the same network.
Keywords: *VPN, DES,3DES, AES,OPNET, IRC, BLOWFISH*

I. Introduction

There are two types of encryption methodologies

1.1 Symmetric encryption

Symmetric encryption also referred to as conventional encryption or single-key encryption was the only type of encryption in use prior to the development of public key encryption in the 1970s.it is a form of cryptosystem in which encryption and decryption are performed using the same key. It is also known as conventional encryption. Symmetric encryption transforms plaintext into cipher text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher text .Traditional symmetric ciphers use substitution and/or transposition techniques. Substitution techniques map plaintext elements (characters, bits) into cipher text elements. Transposition techniques systematically transpose the positions of plaintext elements.

Symmetric encryption scheme has five ingredients (Figure 1):

• Plaintext: This is the original intelligible message or data that is fed into the Algorithm as input.

• Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.

• Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

• Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different cipher texts. The cipher text is an apparently random stream of data and, as it stands, is unintelligible.

• Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the cipher text and the secret key and produces the original plaintext.

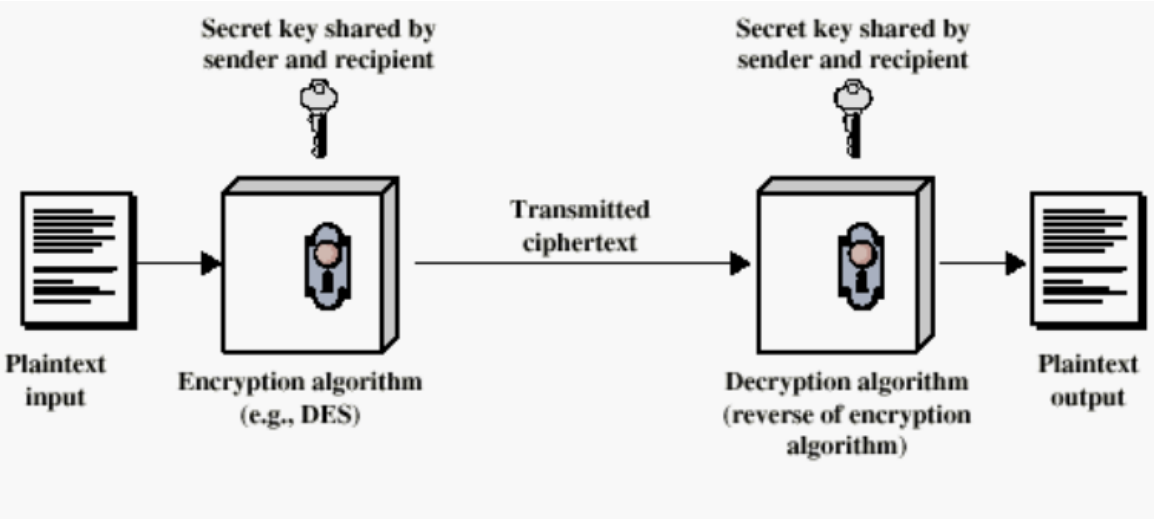

Figure 1. Simplified Model of Symmetric Encryption

Cryptography

Cryptographic systems are characterized along three independent dimensions:

- The type of operations used for transforming plaintext to cipher text. All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext (bit, letter, group of bits or letters) is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost (that is, that all operations are reversible). Most systems, referred to as product systems, involve multiple stages of substitutions and transpositions.
- The number of keys used. If both sender and receiver use the same key, the system is referred to as symmetric, single-key, secret-key, or conventional encryption. If the sender and receiver use different keys, the system is referred to as asymmetric, two-key, or public-key encryption.
- The way in which the plaintext is processed. A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

1.2 Asymmetric encryption

Is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a public key and one a private key. It is also known as public-key encryption. Asymmetric encryption transforms plaintext into cipher text using a one of two keys and an encryption algorithm. Using the paired key and a decryption algorithm, the plaintext is recovered from the cipher text. The most widely used public-key cryptosystem is RSA. The difficulty of attacking RSA is based on the difficulty of finding the prime factors of a composite number

Public-key cryptography provides a radical departure from all that has gone before. For one thing, public-key algorithms are based on mathematical functions rather than on substitution and permutation. More important, public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication.

Terminology Related to Asymmetric Encryption

Asymmetric Keys: Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Public Key Certificate: A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key.

Public Key (Asymmetric) Cryptographic Algorithm: A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pair including the ability to issue ,maintain, and revoke public key certificates.

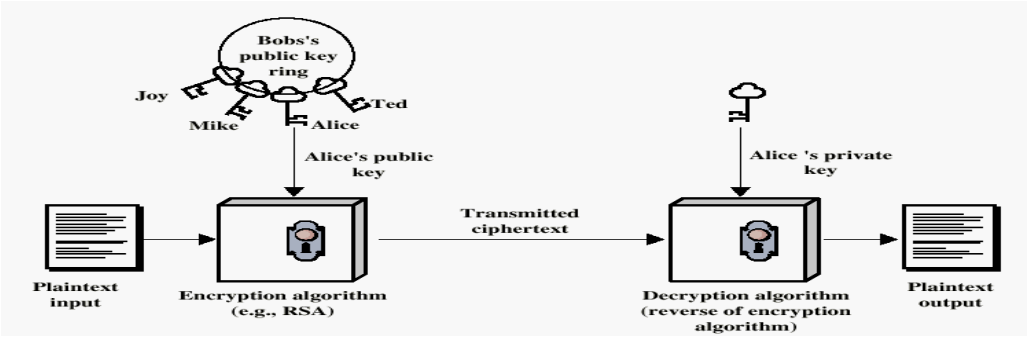

Figure 2. Encryption with public key

• Plaintext: This is the readable message or data that is fed into the algorithm as input.
• Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
• Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
• Cipher text: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different cipher texts.
• Decryption algorithm: This algorithm accepts the cipher text and the matching key and produces the original plaintext.

II. The Design

Four scenarios are used to measure the effect of encryption delay on the network.

In the first scenario the server is accessed by Clients from different three remote LANs connected through IP cloud to the Core router without applying any Encryption (no VPN) as it shown in fig (3). The server supported tow services, DB and HTTP.

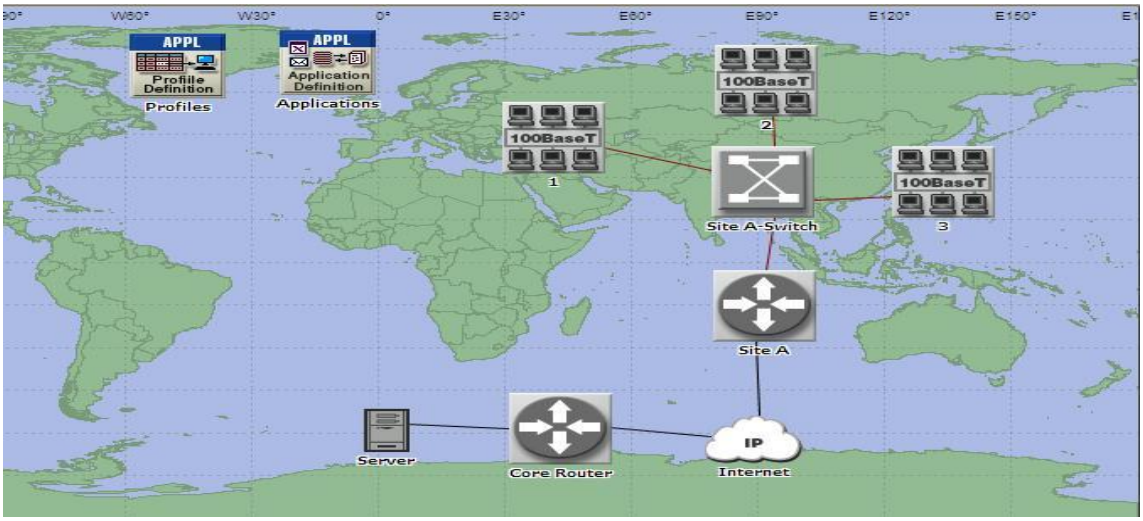

Figure 3.TCP/IP Traffic without Data encryption (No-Encryption Scenario)

In the other three scenarios, encrypted VPN tunneling applied between the three LANs and The Core Router as it shown in figure 4

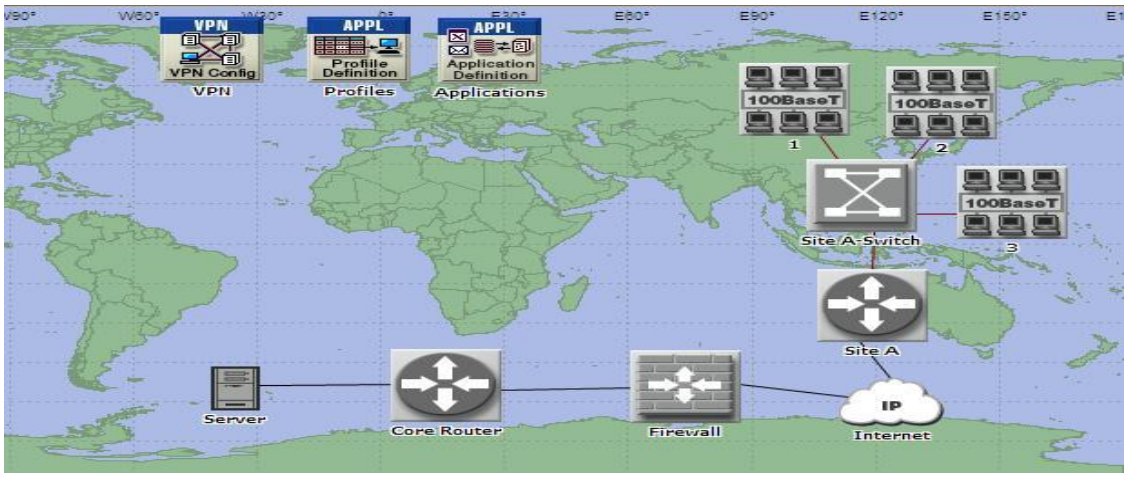

Figure 4. Encrypted VPN Tunnel applied

Encryption/Decryption delay values increased in (Encryption Delay 1, 2, 3) scenarios according to the following table

Scenario	**Encryption/Decryption Delay(ms)**
Encryption Delay 1	0.02 ms
Encryption Delay 2	0.04 ms
Encryption Delay 3	0.05 ms

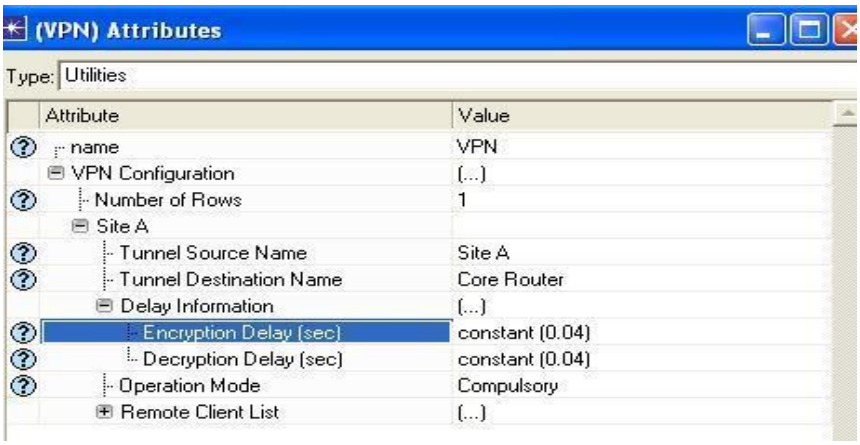

Figure 5. Encryption/Decryption delay setting

III. The Results

An event of the simulation is defined as Web Browsing (Light HTTP), and Database Access (Light). Results were collected after the simulation was run. Statistics of each scenario presented in a graph that detailed the activity throughout the simulation. Graph 6 illustrates the time average (in TCP Delay (Second)).

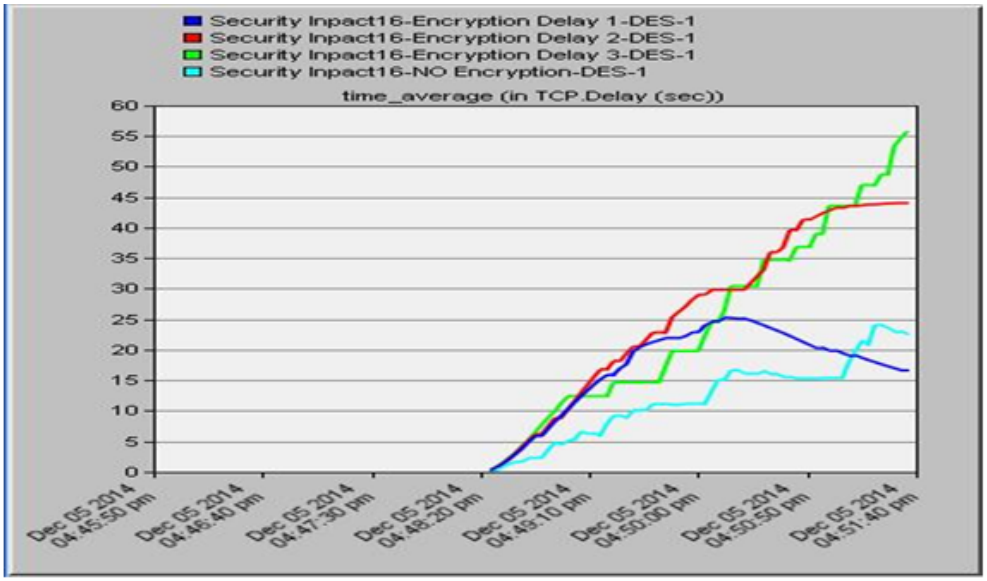

Figure 6. Time_average(in TCP Delay (sec))

The graph shows that the TCP Delay increased simultaneously with the encryption/decryption delay. the lowest value of the delay is before applying encrypted tunnels and the highest value in scenario 3(Encryption Delay 3)which have the highest encryption delay value.

Graph 7 shows the time average (in TCP Segment delay (Sec)).from the graph we remarked that the segment delay also increased according to the increased in encryption delay. Lowest value in NO_ Encryption scenario and highest value in scenario 3(Encryption Delay 3).

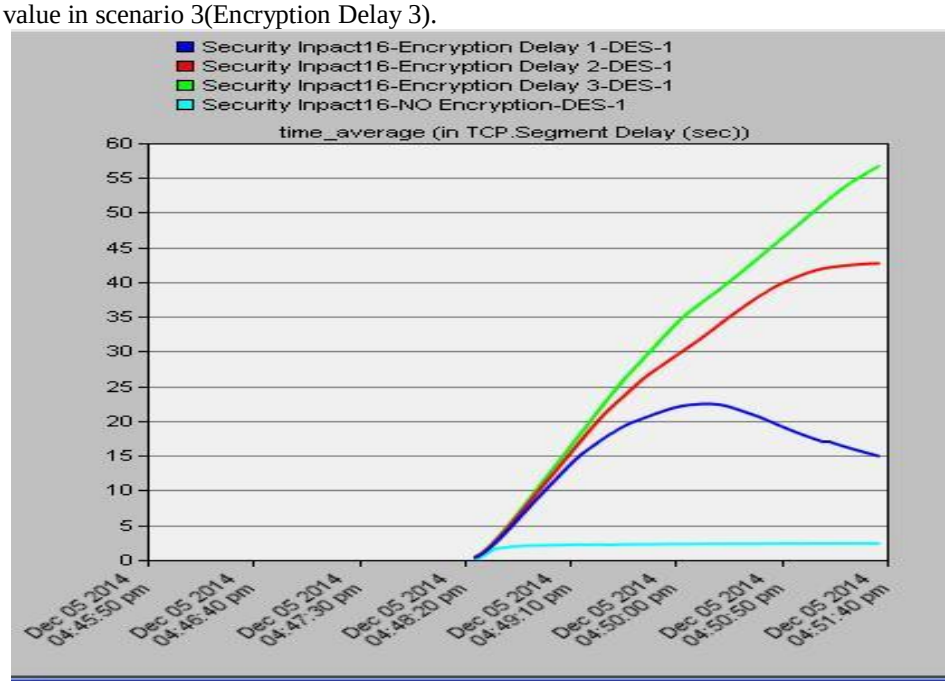

Figure 7. Time average (in TCP segment Delay (sec))

Figure 8 illustrate IP End-to-End delay Variation in the four scenarios. The delay also increased according to the value of encryption Delay.

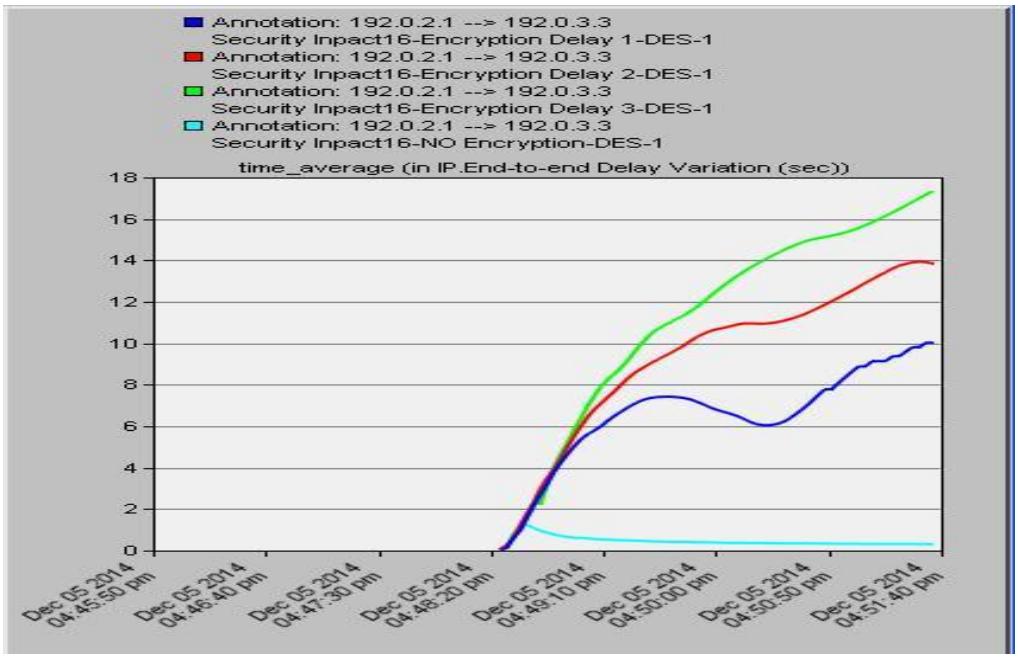

Figure 8. Time_average (in IP End-to-End Delay Variation (Sec))

Figure 9 illustrate the TCP connection Delay. Three scenarios are shown here (Encryption Delay 1, 2, 3 Scenarios).the graph shows that the delay increased forward from scenario 1 to scenario 3.

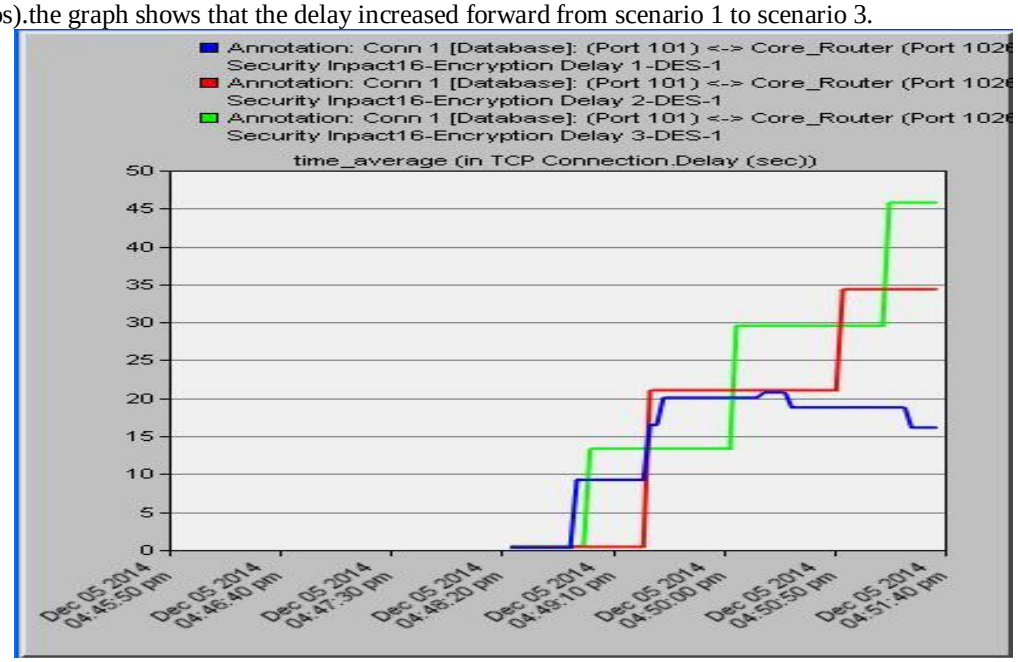

Figure 9. Time_average (TCP connection Delay (Sec))

IV. Conclusion

Referring to the graphs we get that there is a vast TCP Delay after applying the Encrypted tunnels, TCP delay increased according to encryption delay. The Delay on TCP traffic leads to network congestion which affects the performance and stability of the network.

Encryption is the most effective mechanism to secure the flow of data traffic within the network. Encrypted data face some issues. Packet loss, out-of order packets, and TCP latency. Balancing between complex encryption algorithms and performance of the network must is so important to reduce the effect of encryption delay on the network. Using fast encryption algorithms like Blowfish and RC4 when the data is not so important. CPU speed is major part of any encryption system.

References

[1]. Henric Johnson , Network Security, Blekinge Institute of Technology, Sweden.
[2]. W. ~Diffie and E.~Hellman, {New directions in cryptography}, IEEE Transactions on Information Theory {22} (1976).
[3]. Douglas E.Comer, Computer Networks and Internets
[4]. McDysan. D. (2000), VPN applications Guide
[5]. Behrouz A. Forouzan (2007), Data Communications and Networking
[6]. J. Walrand and P. Varaiya, High-Performance Communication Networks.
[7]. Dina Katabi, Mark Handley, and Charlie Rohrs, "Congestion Control for High Bandwidth-Delay Product Networks,"
[8]. David D. Clark, Van Jacobson, John Romkey, and Howard Salwen, "An Analysis of TCP Processing Overhead," IEEE Communications Magazine, June 1989
[9]. Kent, IP Authentication Header, November 1998.
[10]. IPsec VPN WAN Design Overview,http://www.cisco.com
[11]. IPsec Direct Encapsulation Design Guide— http://www.cisco.com/en/US/docs/solutions.
[12]. Kosiur, D,"Building and Managing Virtual Private Networks," New York, NY(1998).
[13]. Erwin, M., Scott, C, Wolfe ," Virtual Private Networks" Sebastopol CA: O'Rielly , Associates Inc(1999).