iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VII **Month of publication:** July 2018

DOI: http://doi.org/10.22214/ijraset.2018.7040

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VII, July 2018- Available at www.ijraset.com

Performance Evaluation Of IPSec Key Exchange Protocol through Simulation

S. Sasikala[1], A. Mohamed Nazeer[2]
[1, 2]*Lecturer, Electrical and Electronics Engineering, PSG Polytechnic College, Coimbatore*

Abstract: ***A secure connection between two hosts in an Internet, Intranet must perform authentication of each endpoint, transport data reliably, protect against tampering or modification of data in transit. The Internet Protocol Security (IPSec) is a standard suite of protocol designed by IETF to provide security for IPv4 and IPv6. IPSec has three sub protocols, namely, Authentication Header (AH), Encapsulating Security Payload (ESP) and Internet Key Exchange (IKE) Protocol. This Paper deals about the performance evaluation of Internet Key Exchange Protocol (IKE v1), heart of IPSec, as it controls the services to be offered to secure the traffic and also manages the range of different transform options. Creation and management of Security Association (SA) are fundamental to the working of IKE and IPSec. The performance of SA at Phase1 and Phase2 is analyzed based on the Packet Size, Bandwidth. The performance measurement parameters include initial SA delay, rekey SA delay of IKE and IPSec. The impact of bandwidth consumption for the average of created SAs ,the delay of creation of SAs and the size of packet exchanged between the different security gateways are simulated and analyzed.***
Index Terms: IPSec Performance, IKE, Internet Security

I. INTRODUCTION

Public and Private networks are susceptible to an unauthorized monitoring and access. Networks are often subjected to an attack. Some attacks are passive, meaning that information is monitored. Others are active, meaning that the information is altered with intent to corrupt or destroy the data or the network itself. Networks and data are vulnerable to attacks [20] such as Eavesdropping , Identity Spoofing ,Data Modification ,Password-Based Attacks, Denial-of-Service Attack, Man-in-the-Middle Attack, Sniffer Attack, Application-Layer Attack if no security plan in place. Computer networks are utilized for sharing services and resources. Information traveling across a shared IP-based network, such as the Internet, could be exposed to many devious acts such as eavesdropping, forgery and manipulation. So information need to be sent in a secure manner to the trusted receiver. IP-based networks divides data into packets and the independent routing of packets through a large network with no central control. Each packet is marked with its sender and receiver, the packets are not invisible to other devices on the network. An intermediate network device can easily intercept and examine any passing packet. This property of IP-based networks creates several potential security problems.

The Internet Protocol suite [17] provides no security at all. Security protocols can be utilized on all layers in the protocol suite to protect data in different ways. Designers proved that the IP layer is a good place to secure the data being communicated. Reasons are the IP layer is at the choke point of Internet communication can capture all packets sent from the higher-layer protocols and applications and all packets received by the lower-layer network protocols. Security provided at this layer is independent of lower-layer protocols. Security provided at this layer can be made transparent to the higher-layer protocols and applications. Many application environments can benefit from security provided at the IP layer. The Internet Protocol Security (IPSec) suite [6] [7] to provide network security services such as confidentiality, data origin authentication, data integrity and anti-replay to protect datagrams in the Internet. Internet Key Exchange (IKE) is one major component in IPSec which deals Key Management [14] [15] [18] aspects. IKE allows communicating entities to derive session keys for secure communication via a series of exchange of messages. This work deals about performance of IKE v1. Due to scalability and practical implementation considerations, automatic key management seems a natural choice for exchange of messages in significantly large Virtual Private Networks (VPNs).

II. INTERNET PROTOCOL SECURITY

IPSec provides security at the network layer. The objectives are met through the use of two traffic security protocols, the Authentication Header (AH) [8] [9] and the Encapsulating Security Payload (ESP) [10], and through the use of cryptographic key management procedures and protocols. IPSec may be used in three different security domains - Virtual Private Networks, application level security, and routing security as shown in Fig.1

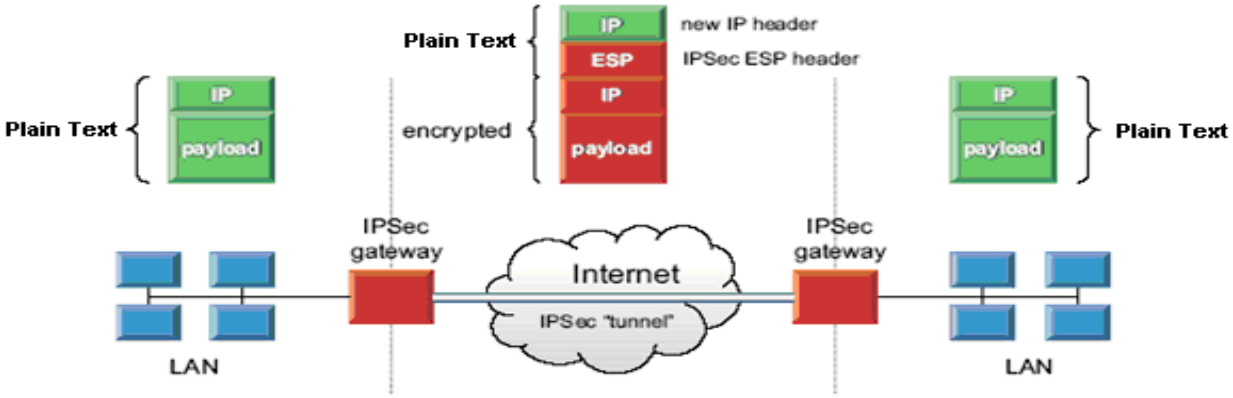


Fig. 1 VPN using IPSec

Fig. 2 shows the IPSec Components. It has two core protocols, namely, IPSec protocols, Internet Key Exchange protocol. The IPSec protocols are the protocols used to protect the actual traffic being passed through the VPN. The actual protocols used, and the keys used with them are negotiated by IKE. There are two protocols associated with IPSec, namely, AH and ESP.

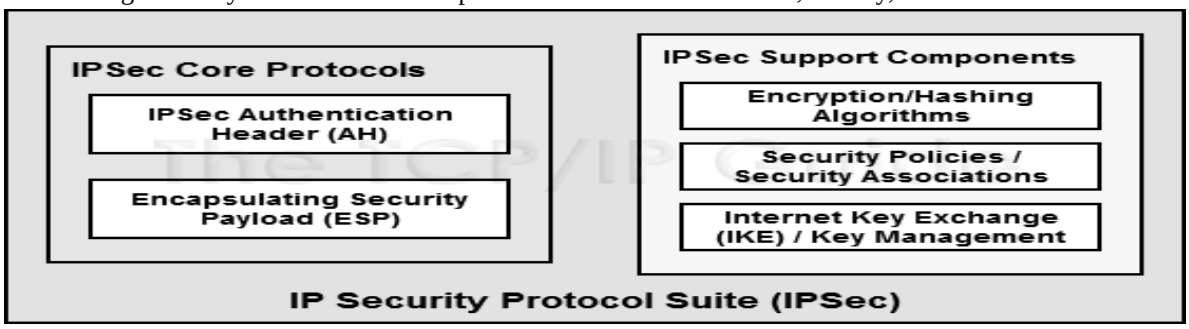


Fig. 2 IPSec Protocols and Components

The **I**nternet **K**ey **E**xchange protocol [3] [4] is a key management protocol standard that is used in conjunction with the IPsec standard. It is a hybrid protocol that integrates the Internet Security Association and Key Management Protocol (ISAKMP) [11], Secure Key Exchange Mechanism (SKEME) [3] [11], Photuris, and a subset of the Oakley key exchange scheme [11]. The purpose of IKE is to allow devices to exchange information required for secure communication. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations. It is an IPSec automated key management protocol. IKE eliminates the need to manually specify all the IPSec security parameters. The Ike Functions are to Provide a means for the endpoints to authenticate each other, establish new IPsec connections and manage existing connections. The process of negotiating session parameters consists of a number of phases and modes. IKE parameters such as Tunnel / Transport mode, Main/Aggressive Mode, IPSec Protocols IKE Encryption, IKE Authentication, IKE Diffie-Hellman Group, IKE Lifetime, IPSec Encryption, IPSec Authentication, IPSec Lifetime [14] [18] are used in the negotiation process.

III. SIMULATION DESIGN

This simulation design deals about the elements used to create a DML definition for a network, the experimental environment considered for the analysis of IKE performance and the design flow. The network is modeled using DML. The Security configurations are put in place using NIST IPSec and IKE Simulation tool. IKE Performance Issues are SA Establishment Latency [14] [18], a measure of time taken to setup an SA by the initiator, IKE SA Phase 1 : Initial & Rekey, IPSec SA Phase 2 : Initial & Rekey. SA lifetime, a time interval after which an SA must be replaced with a new SA expressed as time or byte count. Phase 1 SA Rekeying**,** Continues Channel Mode or Non-Continues Channel Mode. Performance Metrics includes VPN's dimensions , bandwidth, packet size. This simulation work deals about the performance impact based on the bandwidth, packet size as the metrics.

IV. SIMULATION TESTING AND RESULTS

The testing parameters considered for this work and its result are

Table 1 IPSec and IKE Parameters

Variable	Default Value
Encryption algorithm	THREE_DES_CBC
Authentication algo.(IKE/IPsec)	HMAC_SHA1
Lifetime (IKE)	1000 seconds
Lifetime (IPSec)	400 seconds
Simulation duration	172800 seconds (48 hours)
link delay	50 ms
network interface delay	0 ms
bandwidth (between gateways)	1.5 Mbps
bandwidth (gateway and host)	100 Mbps
Threshold (initiator)	85%
Threshold (responder)	90%

The results are analysed for the simulated model of DML program.

Graphical Network View of simulated network model

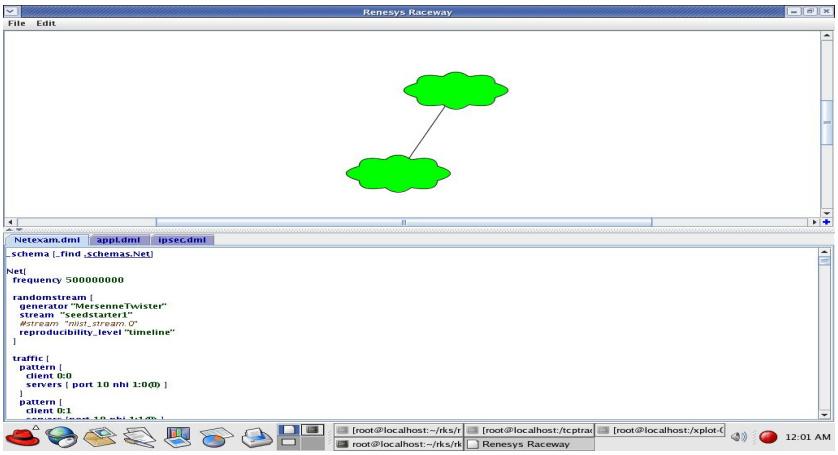


Fig. 4 Graphical screen of simulated network Model

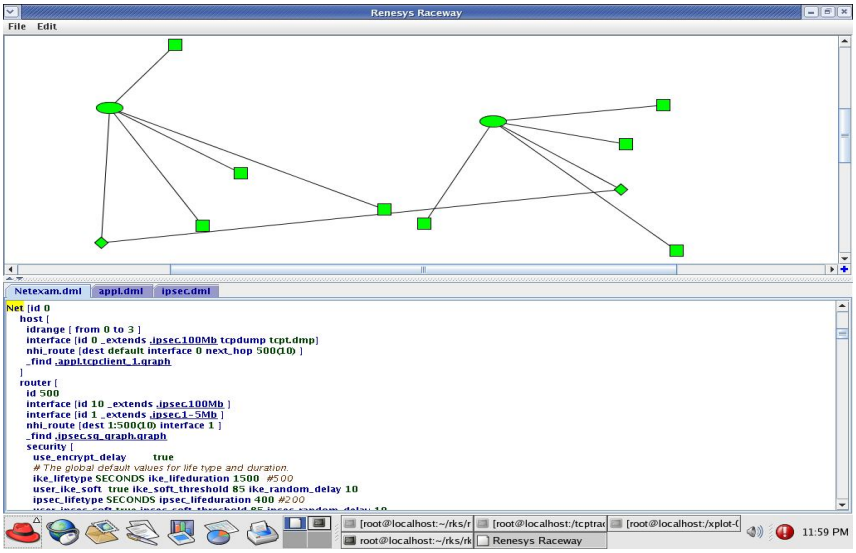


Fig. 5 Networks with Hosts Screen

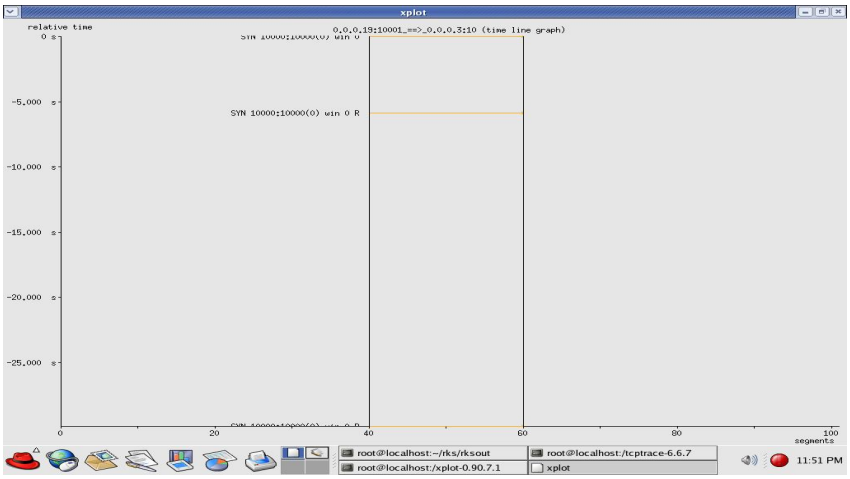


Fig. 3 Timeline Graph Screen

Experiment-1: Influence of Router Bandwidth and Data Transfer Rate for the Host Bandwidth-100 Mbps, IKE Life duration -1000 s, IPSec Lifetime- 400 s, IPSec Timer interval-2s, IKE Timer interval- 2 s, the values are interpreted from running a model.

Table 2 Router Bandwidth: 1.5 Mbps

Interface Latency	Duration (in Seconds)	Data Transfer Rate (in KBps)
0.0	21.076	1639
0.5	11.423	3025
0.8	10.699	3230
1.0	136.369	3253
10	11.349	2947
100	11.727	2947
1000	11.166	3095

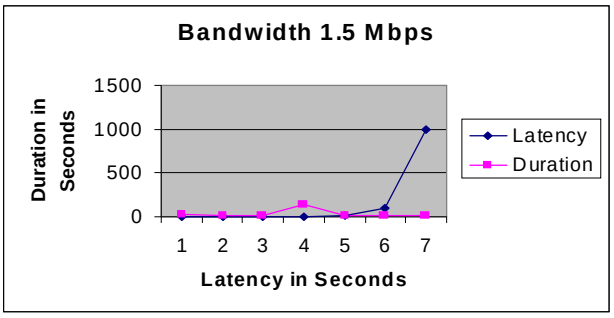


Fig. 6 Latency vs Duration

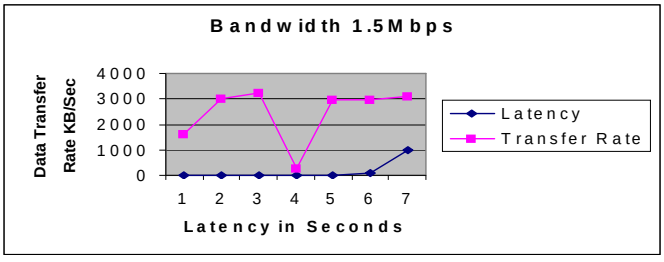


Fig. 7 Latency vs data transfer rate

I**nference**: With increase in Interface latency data transfer rate increases and exceptional behaviour was noted when the Interface latency was 1.0 for 1.5 Mbps bandwidth.

Table 3 Router Bandwidth: 10 Mbps

Interface Latency	Duration (in Seconds)	Data Transfer Rate (in KBps)
0.0	10.18	3395
0.5	10.5	3291
0.8	10.177	3396
1.0	10.5877	3264
10	10.696	3234
100	10.738	3218
1000	12.788	2702

Inference: As the Interface latency increases the data transfer rate decreases.

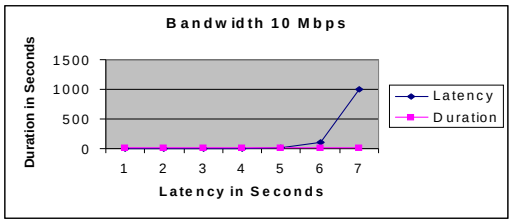


Fig. 8 Latency vs Duration

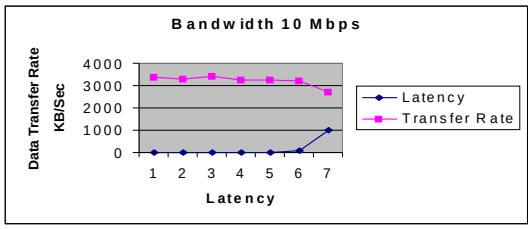


Fig. 9 Latency vs Data transfer rate

Table 4 Impact on Bandwidth

Bandwidth (in Mbps)	Duration (in Seconds)	Data Transfer Rate (in KBps)
1.5	10.81	3214
10	30.5	2448
100	23.5	2444

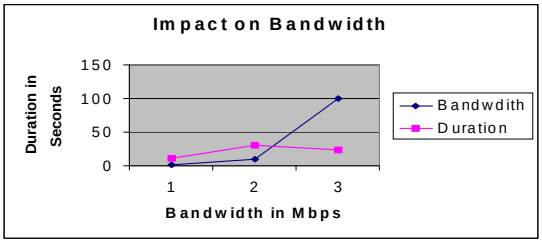


Fig. 10 Bandwidth vs duration

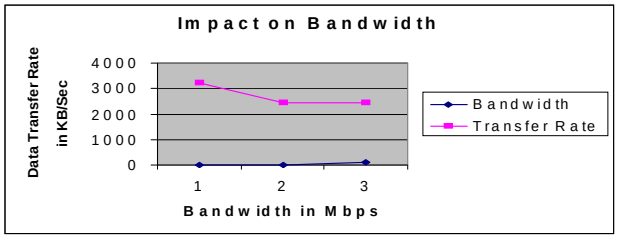


Fig. 11 Bandwidth vs data transfer rate

Experiment-2 To measure the influence of Bit rate speed for various Bandwidths, the Bit rate was studied for 100, 1000, 10000 against 1.5 Mbps, 10 Mbps, 100 Mbps router with latency 0. IPSec timer interval 2s.
Router Bandwidth: 1.5 Mbps

Table 5 Bitrate Vs Data Transfer Rate: 1.5 Mbps

Interface Bit Rate	Duration (in Seconds)	Data Transfer Rate (in KBps)
100	11.561	2989
1000	11.132	3104
10000	11.179	3191

Inference: Data transfer rate Increases with Bitrate for 1.5 Mbps
Router Bandwidth: 10 Mbps

Table 6 Bitrate Vs Data Transfer Rate: 10 Mbps

Interface Bit Rate	Duration (in Seconds)	Data Transfer Rate (in KBps)
100	10.757	3213
1000	10.901	3190
10000	10.887	3174

Inference: As the Bit rate increases the Data transfer rate decreases.
Router Bandwidth: 100 Mbps

Table 7 Bitrate Vs Data Transfer Rate: 100 Mbps

Interface Bit Rate	Duration (in Seconds)	Data Transfer Rate (in KBps)
100	11.297	3059
1000	19.219	1898
10000	18.651	1853

Inference: As the Bit rate increases the Data transfer rate decreases.
Experiment-3
This experiment is about study of the influence of IPSec timer interval to the Network**.**

Table 6.7 Influence of IPSec timer interval

IPSec Timer Interval in Seconds	Total Records Used	Total Bytes	Duration (in Seconds)	Data Transfer Rate (in KBps)
0.1	3456025	691204208	195.196	1.359
100	3481	695408	1.994	348
1000	371	73408	1.708	42
10000	61	11408	1.359	8

Inference: As the IPSec timer interval increases with the Data transfer rate increase.

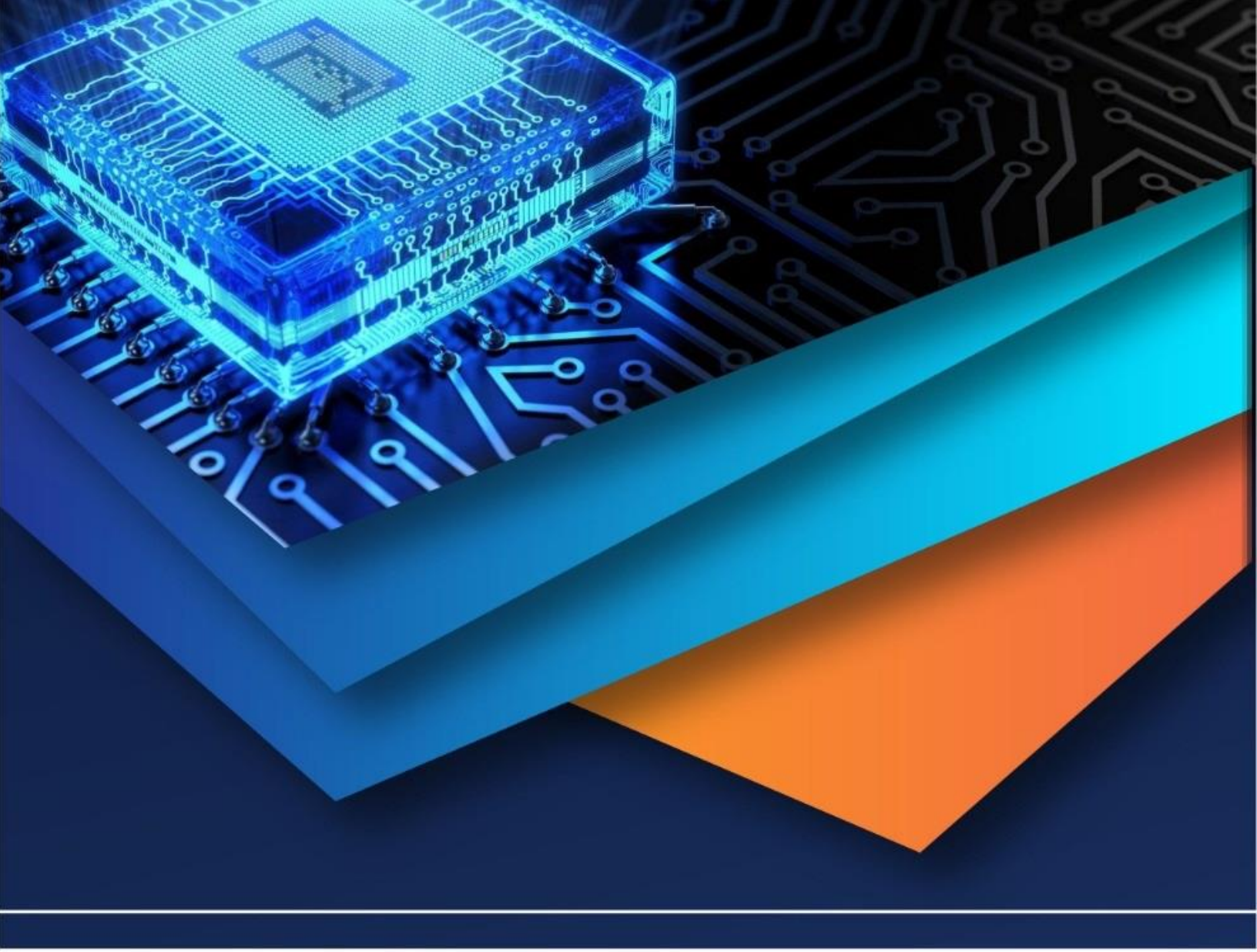
III. CONCLUSION

The security attribute values and the experiment-specific parameter values can affect the overall performance and dynamics of security protocol operations. The values of one or more parameters are changed to see what affect those parameters and their values play on performance**.** A security gateway initiates the SA negotiation for both IKE and IPSec on a need basis. Packet statistics represent counts of various packet types processed at the IPSec module such as protected/unprotected/bypassed/error packets. The IP packets are counted for both inbound and outbound independently within a security gateway. The impact on bandwidth for different parameters like latency, bitrate, IPSec interval are observed. The inferences are increase in bandwidth results in decrease in data transfer rate due to the encryption, authentication process. Increase in bit rate decreases the data transfer rate. For higher time interval the data transfer rate decreases. It was found that the optimal time interval should be lower. For the smaller network the

impact on packet size, SA latency, rekey, does not give variations. These impacts have been studied using the default encryption, authentication used for the IPSec key management. This study can be extended to give efficient protection against packet at the time of communication by using various efficient algorithms, high speed processors.

REFERENCES

[1] Perlman R., Kaufman C., "Key Exchange in IPSec: Analysis of IKE", IEEE Internet Computing Journal special issue on Security Solutions, vol. 4, no. 6, pp. 50--56, Nov/Dec 2000.
[2] Soussi H., Hussain M., Afifi H., Seret D., "IKEv1 and IKEv2: A Quantitative Analyses", WEC'05 Conference one security information, Istanbul, Turkey, 24 June 26, 2005.
[3] Okhee Kim, Doug Montgomery, "Behavior and Performance Characteristics of IPSec/IKE in Large Scale VPN's", IASTED International conference on communication, network, and information security, Dec 10 –12, 2003.
[4] Carlton R. Davis, " IPSec: Securing VPNs", Tata McGraw-Hill, New Delhi, 2001.
[5] Douglas E. Comer, "Internetworking with TCP/IP", Printice Hall of India, New Delhi, 2003.
[6] John Mairs, "VPNs A Beginner's guide", Tata McGraw-Hill, New Delhi, 2002
[7] Richard Blum, "Network Performance Open Source Toolkit", Wiley Publishers, India, 2003
[8] Richard E. Smith, "Internet Cryptography", Addison Wesley, Second Indian Reprint , 2000.
[9] William Stallings, " Cryptography and Network Security", Printice Hall of India, New Delhi, 2004.
[10] Harkins D., Carrel D., "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
[11] Hoffman P., "Algorithms for Internet Key Exchange version 1 (IKEv1) ", RFC 4109, May 2005.
[12] Kent S., Atkinson R., "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
[13] Kent S., Seo K., "Security Architecture for the Internet Protocol ", RFC 4301, December 2005.
[14] Kent S., Atkinson R., "IP Authentication Header", RFC 2402, November 1998.
[15] Kent S., "IP Authentication Header", RFC 4302, December 2005.
[16] Kent S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
[17] Maughan D., Schertler M., Schneider M., Turner J., "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
[18] McDonald D., Metz C., Phan B., "PF_KEY Key Management API, Version 2", RFC 2367, July 1998.
[19] "SSFNET and DML Reference Manual", www.ssfnet.org
[20] "NIIST IPSec / IKE Simulation tool", www.antd.nist.gov/niist



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY