ABUAD Journal of Engineering Research and Development (AJERD) ISSN: 2645-2685
Volume 2, Issue 2, 43-49

An Assessment of the Performance of IPsec Internet Key Exchange in Aggressive and Main Mode

Emmanuel Adewale ADEDOKUN[1], Mohammed Bashir MUA'ZU[1], Alice Ochanya LAWRENCE[1], Habeeb Bello SALAU[1]

[1]*Department of Computer Engineering, Ahmadu Bello University, Zaria, Nigeria*
wale@abu.edu.ng/mbmuazu@abu.edu.ng/alochanya@abu.edu.ng/bellosalau@abu.edu.ng

Corresponding Author: alochanya@abu.edu.ng

Date Submitted: 10/06/2019
Date Accepted: 06/10/2019
Date Published: 31/12/2019

Abstract*: One of the most widely accepted security schemes in virtual private networks (VPN) is the Internet protocol security (IPsec) tunnelling protocol. The choice of modes for the implementation of this scheme depends on application requirements. As crucial as this may be, oftentimes the specific mode in which this IPsec Internet key exchange (IKE) is implemented is not being specified. In this paper, we present a framework for the implementation of IPsec IKE in both aggressive and main mode towards appreciating the necessity for specifying the mode of implementation by researchers and the implications for doing so. IPsec IKE tunnelling protocol was configured in aggressive and main modes using encapsulating security protocol (ESP) protocol in tunnel mode in a site to site VPN architecture. The network was designed and implemented in graphical network simulator 3 (GNS3) using Cisco devices. The network was analysed using Wireshark network analyser. The performance of both networks was measured using throughput and latency. Experimental results showed an improved average performance of about 0.5% and 11% recorded by the aggressive mode over the main mode in terms of throughput and latency respectively. Though, the aggressive mode performs better, it may not always be suitable for all systems, however, it is best suited for any message that does not require encrypted authentication and could thus be configured for site to site implementations when optimal security is not a major concern. Our findings attest to the fact that there is need to specify the mode of implementation of any IPsec IKE tunnelling protocol and the associated implication, thereby, avoiding erroneous decisions by network engineers.*

Keywords: *aggressive mode, ESP, IKE, IPsec, main-mode, and tunnel*

1. INTRODUCTION

Virtual private networks (VPN) provides the opportunity for the provision of secure end to end connections through tunnelling technologies (Forouzan & Mukhopadhyay, 2011; Shrivastava & Rizvi, 2014; Wu, 2009). This guarantees security and privacy of transmitted IP packets over public networks, using advanced encryption and authentication algorithms (C. A. Shue *et al.*, 2007; Wu, 2009). VPN offers a secure, scalable, and cost-effective means of providing security across public networks when compared to direct or leased lines (Ismoyo & Wardhani, 2016; Lammle, 2011; Lu & Dong, 2011).

The deployment of VPN tunnels over public networks depends on application requirements (Jahan *et al.*, 2017). Of particular importance during such network deployment is providing necessary associated information that includes being specific on the type of protocol used, associated components as well as area of deployment. Such information will provide the necessary guide towards understanding the network design, as well as ease of carrying out necessary maintenance on the network when the need arises. However, most tunnelling protocol specifically the Internet protocol security (IPsec) reportedly designed and implemented in literature are not being specific on the mode in which the proposed IPsec protocol is being deployed as well as associated components required for such deployment (Rao *et al.*, 2015; Smaoui *et al.*, 2012; Yasinovskyy *et al.*, 2009).

Often times, researchers implement the IPsec tunnelling protocol on networks without key components that guarantee security of the network, deployment without the needed encryption as well as non-referencing of the encryption or authentication properties used on the tunnel (Rao *et al.*, 2015; Yasinovskyy *et al.*, 2009). Thus, it becomes pertinent to present methods and findings from research in unambiguous manners towards aiding its understanding, replication as well as managing the network, which serves as the motivation for this study.

The main contribution of this paper is to describe and analyse the implementation of IPsec Internet key exchange (IKE) in main and aggressive modes using the encapsulation security payload (ESP) protocol in tunnel mode on a site to site VPN architecture. By default, IPsec main mode is configured on a site to site VPN architecture while IPsec aggressive mode is configured in a remote access VPN architecture (Jahan *et al.*, 2017; C. Shue *et al.*, 2005; Singh *et al.*, 2012). The rest of the paper is structured as follows: Section 2 presents the related work. While, section 3 presents the network design and experimental setup for the implementation of the IPsec IKE protocol. Section 4 presents and analysed the results obtained in implementing the proposed design in both aggressive and main modes. While, conclusion is drawn in section 5.

2. REVIEW OF RELATED WORKS

Some achievements presented in literature that motivated this study is presented in this section. We note that a major drawback with most IPsec tunnelling protocol approach reported is failure to explicitly state the mode in which the IPsec protocol is being implemented as well as the associated component. This ambiguity tends to confuse the network engineer and other researchers in understanding the network, towards making useful analysis and decision. An IPsec protocol was implemented on Windows 2003 operating system (OS) using Cisco equipment in (Wu, 2009). Despite giving highlights of the IPsec properties, the specific mode in which the protocol was implemented was not stated or the area of deployment. Similarly, an IPsec tunneling protocol was used in securing internetworks of the third-generation partnership project (3GPP) in (Smaoui *et al.*, 2012). This includes the long-term evolution (LTE) and wireless local area network (WLAN). Mobility and multihoming protocol (MOBIKE) was used to provide mobility extension to the IKEV2 towards ensuring the re-establishment of the security association (SA) between the networks. However, the IPsec components such as ESP or authentication header (AH) protocol utilized for the implementation was not stated. Also, the authors failed to state if the mode of operation was either in transport or tunnel mode. Furthermore, the mode of implementation of the IKE was not provided.

An Openswan IPsec implementation approach was presented in (C. A. Shue *et al.*, 2007; Yasinovskyy *et al.*, 2009). The proposed approach was successfully implemented. However, the component of the Openswan IPsec utilized was not stated. Similarly, IPsec protocol using AH in field programmable gate array (FPGA) for internet of things (IoT) was implemented in (Rao *et al.*, 2015). The scheme was designed to provide data authentication as security to IoT applications using the AH protocol and secure hash algorithm -3 (SHA3). Though, it has been established in literatures that using AH protocol lacked the required confidentiality which is a property of encryption. Thus, it cannot guarantee data security (Ha *et al.*, 2004) .

A performance evaluation of VPN protocols in Windows 2003 environment using IPsec, point to point tunneling protocol (PPTP), and secure socket layer (SSL) was presented in (Narayan *et al.*, 2008). Results obtained showed that throughput in a VPN tunnel could range between 40 – 90 Mbps depending on three factors namely, the chosen protocol, the algorithm used, and the Window size which in turn affects the central processing unit (CPU) utilization of VPN servers. Although, triple data encryption standard (3DES) and message digest 5 (MD5) were stated to have been used for the encryption and hashing in the IPsec tunnel, they were not clear on the mode of implementation or the protocol used.

Also, IPsec AH and ESP protocols in tunnel and transport modes in system on chips (SoC) was proposed in (Niu *et al.*, 2011). This entailed the utilization of advanced encryption standard (AES) and SHA encryption and hashing algorithms respectively. The system was designed for a high performance in-line network security processor that integrates two embedded 32-bits CPU cores and IPsec processor on SoC. However, implementing IPsec in AH does not guarantee confidentiality of transmitted pack (Ha *et al.*, 2004; Kent & Atkinson, 1998). Also, the IKE mode used for the implementation was not stated.

An end to end secure connection in 6LoWPAN based on the configuration of IPsec tunnel was presented in (Raza *et al.*, 2011). IPsec implementation in ESP and AH protocols was examined. Nevertheless, the IKE implementation mode was not stated. Hence, making it difficult for researchers to replicate such design as well as examining the performance of such implementation.

3. PROPOSED DESIGN AND EXPERIMENTAL SETUP

This section presents the proposed methodology used in the network design and the implementation of IPsec IKE in main and aggressive modes. The overall design process flow is summarized in Fig. 1. The network was designed and configured in GNS3 network simulator installed on HP Laptop, (Intel ® Core(™) i5-7200 CPU @2.70GHz, 64 –bits Operating System, x64-based processor, 1-TB HDD, 8GB RAM. The design parameters used for the emulation is presented in Table 1. An IPsec IKE tunnel in main and aggressive mode was implemented based on the network topology presented in Fig. 2. This is a site to site VPN architecture. Data packets were injected into the designed network towards analysing their performance in terms of latency and throughput in each of the implementation mode using a Wireshark network analyser. Packets were injected until maximum transmission unit (MTU) was reached. Thus, defragmented packets were not considered. The choice of these metrics for evaluation purpose is attributed to the consensus of researchers that a robust network must have a considerable high level of throughput with small latency (Narayan *et al.*, 2008; Narayan *et al.*, 2015; Santos & Stuppi, 2015). The throughput is the rate of successful packet delivery per seconds over a communication medium as expressed in (1). While, latency is associated with the minimal time spent in transmitting packets from source to destination within the designed network.

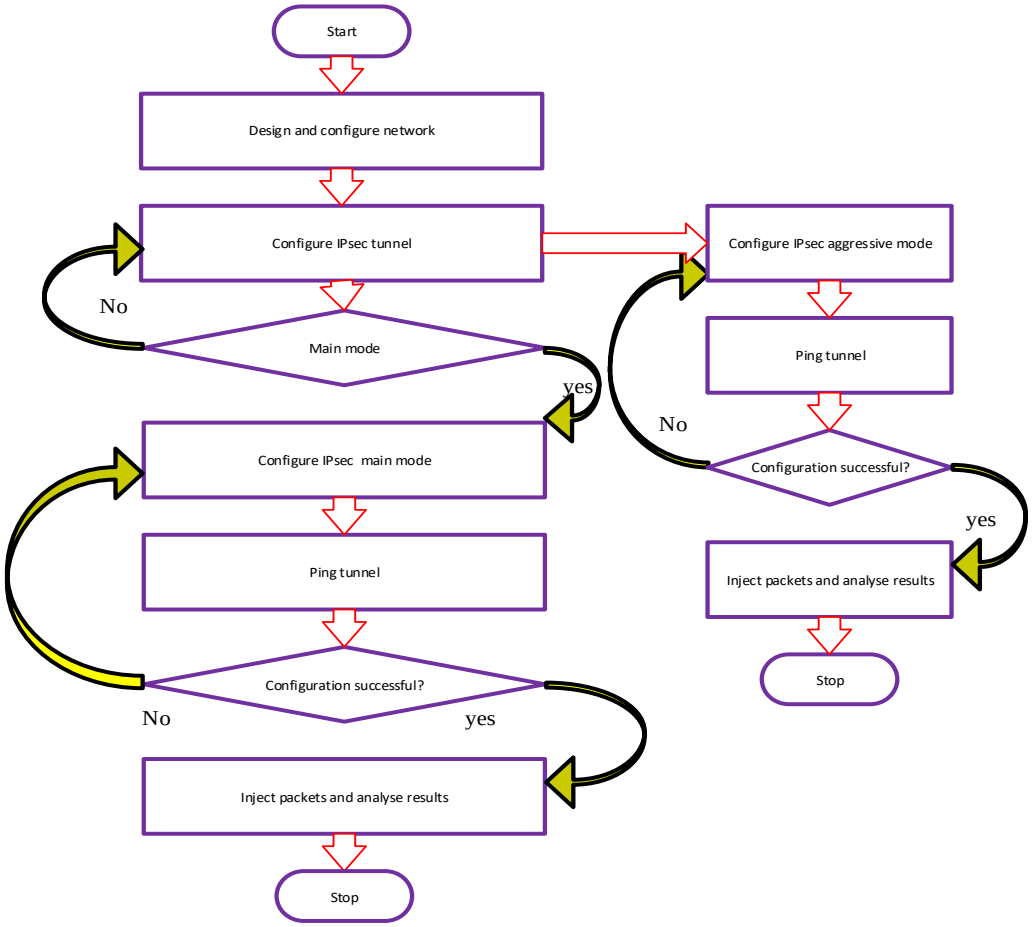

Fig 1: Fig.1: Flowchart of the experimental setup

$$\text{Th} = \frac{Ps}{\text{L}} \quad (1)$$

where Th is the throughput measured in bps, PS is the packet size measured in byte and L is the latency measured in ms.

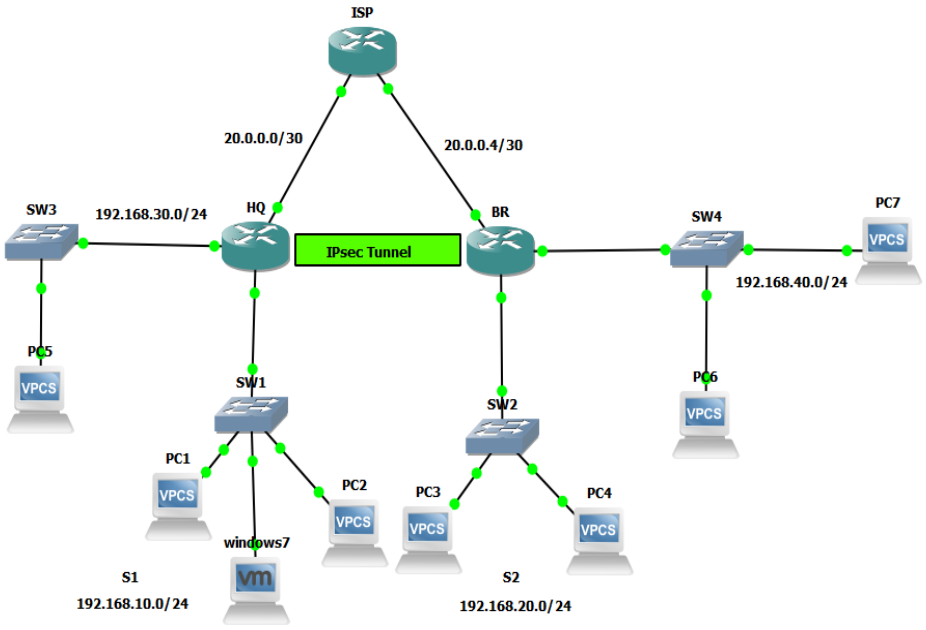

Fig 2: Design network topology

An IPsec tunnel was setup between the head office (HQ) and the branch office (BR) to provide security to applications on end devices on S1 and S2 networks. It is worthy to note that the ISP router is unaware of the existence of the tunnel between the two communicating sites, HQ and BR as seen in Fig. 2. The end devices were connected to the C7200 routers on the communicating sites using Cisco 8-ports Ethernet switches. The Window 7 operating system (OS) is a virtual machine (VM) installed on a VMWare and it served as the network server (See Fig. 2). Other network parameters used in the network design and experimental set-up are summarized in Table 1.

Table 1: List of emulation parameters

S/N	Parameter	Value
1	Simulation software	GNS3 2.03
2	Router	Cisco router C7200
3	Switch	Cisco 8-port Ethernet switch
4	Operating system	Windows 7 (VM)
5	Routing protocol	OSPF
6	Encryption algorithm	AES 256
7	Hashing algorithms	SHA 256
8	VMWare	Ubuntu 14.04 LTS
9	Computers	VPCs

4. RESULTS AND DISCUSSIONS

The experimental result obtained from the implementation of the IPsec IKE in both main and aggressive modes based on the proposed methodology and emulation parameters presented in Table 1 is presented in this section. We observed generally on the average that the implementation in the aggressive mode showed a better performance in terms of throughput and latency compared to that of the main mode (see Fig.3 and Fig.4) respectively. This can be attributed to the encryption overhead in the main mode since it uses more packets for negotiating the proposal for the establishment of the security association compared to the aggressive mode which uses fewer packets. An average performance improvement of about 0.5% was recorded interms of throughput in the aggressive mode compared to main mode (Fig. 3).

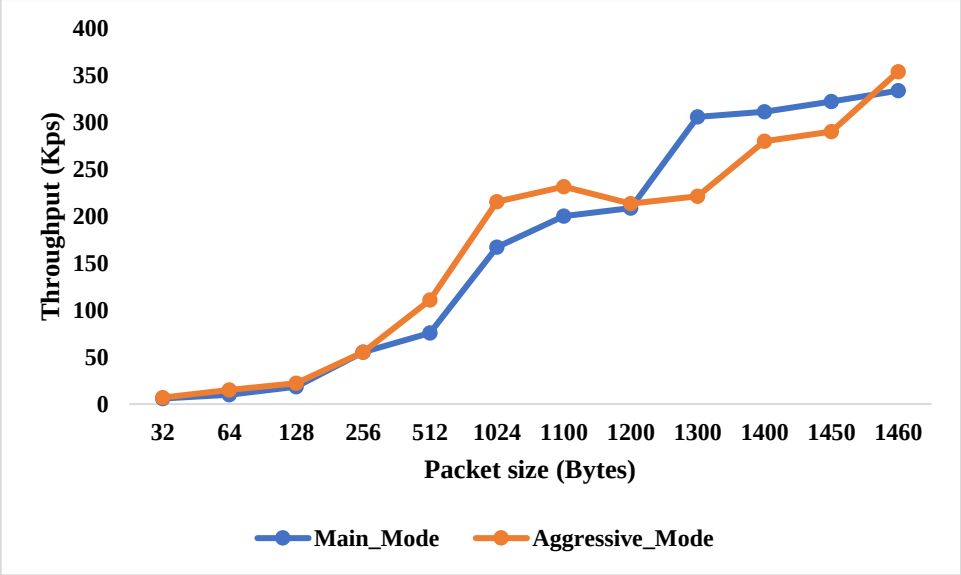

Fig 3: Fig 3: Graph of throughput against packet size

A similar trend was observed in Fig. 4 that on the average, the aggressive mode recorded a lower latency compared to the main mode with about 11% reduction. We note that as packet size approaches MTU, the computational time began to decrease in the aggressive mode and the throughput began to rise. Surprisingly, we observed that at about 1200bytes to 1450bytes as packets size approach MTU, the main mode tends to perform better than the aggressive mode in terms of increased throughput as well as reduced latency compared to the aggressive mode (see Fig 3&4 respectively). Though, we associate this trend to a possible linear incremental pattern of packets injected into the network; area of deployment, as from literature, IPsec main mode is configured basically for site to site VPN which is the mode of implementation in this work while aggressive mode is mostly configured for remote access VPN; the CPU utilization, as VPN servers are CPU dependent and consume resources and this affects throughput; and, the TCP maximum segment size (MSS) which also affects IPsec performance. However, effort is still ongoing towards investigating the possible reasons for this observed pattern beyond the stated reasons.

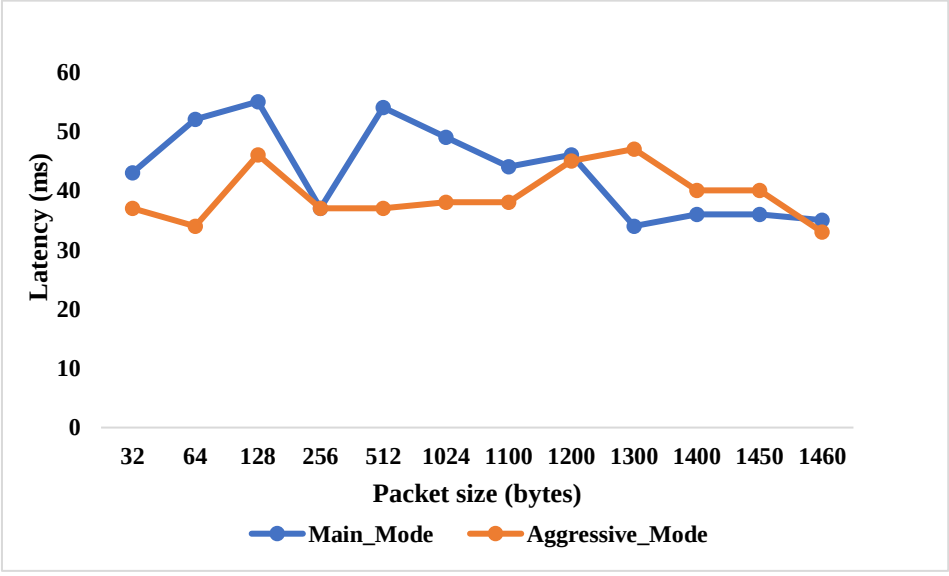

Fig 4: Graph of latency against packet size

5. CONCLUSION AND RECOMMENDATION

This paper presents the implementation of IPsec IKE in main and aggressive modes. The designed network was emulated in GNS network simulator using Cisco devices. It was observed that the implementation in aggressive mode showed a better average performance in terms of throughput and latency with about 0.5% and 11% respectively. Though the aggressive mode which up until now is configured majorly for remote access VPN performs better for all metrics considered than the main mode, it may not always be suitable for all systems. However, it is best suited for any message that does not require encrypted authentication. If authenticated encryption is not a major requirement on a site to site VPN architecture, IPsec aggressive mode could be configured for improved network performance against its stringent use in remote access VPN. We note that this effort is geared towards the campaign for the need for researchers to specify the kind of modes in which the IPsec protocol is being implemented, area of deployment as well as the associated component. This will be useful to engineers and researchers in the field in understanding, analysing, and possible replication of the network. Future research effort will focus on investigating the possible reason for the sudden improved performance observed in terms of throughput and latency at higher packet size of 1200bytes to 1450bytes in the main mode. In addition, the packet behaviour through the tunnel for the IKE implementation in both aggressive and main mode will be further analysed.

REFERENCES

[1] Forouzan, B. A., & Mukhopadhyay, D. (2011). *Cryptography and Network Security (Sie)*: Special Indian Edition, McGraw-Hill Education.

[2] Ha, C.-S., Lee, J. H., Leem, D. S., Park, M.-S., & Choi, B.-Y. (2004). ASIC design of IPSec hardware accelerator for network security, in *Proceeding of 2004 IEEE Asia-Pacific Conference on Advanced System Integrated Circuits*, 2004, paper 0-7803-8637-X/04, 168-171

[3] Ismoyo, D. D., & Wardhani, R. W. (2016). Block cipher and stream cipher algorithm performance comparison in a personal VPN gateway, in *Proceeding of Technology of Information and Communication (ISemantic), International Seminar on Application for Technology of Information and Communication*, 2016, ISBN 1509023267, 207-210

[4] Jahan, S., Rahman, M. S., & Saha, S. (2017). Application specific tunneling protocol selection for Virtual Private Networks, in *Proceeding of 2017 International Conference on Networking, Systems and Security (NSysS)*, 2017, paper 978-1-5090-3260-0/17, 39-44

[5] Kent, S., & Atkinson, R. (1998*). IP Authentication Header* RFC 2402 (Proposed Standard).

[6] Lammle, T. (2011). *CCNA Cisco Certified Network Associate Deluxe Study Guide*: John Wiley & Sons.

[7] Lu, J., & Dong, C. (2011). Study on the application of VPN technology based on IPSec in the modern universities in *Proceedings of 2011 IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS)*, 2011. ISBN 1424496985, 881-883

[8] Narayan, S., Kolahi, S. S., Brooking, K., & de Vere, S. (2008). Performance evaluation of virtual private network protocols in Windows 2003 environment, in *Proceeding of 2008 International Conference on Advanced Computer Theory and Engineering*, 2011. Paper 978-0-7695-3489-3/08, 69-73

[9] Narayan, S., Williams, C. J., Hart, D. K., & Qualtrough, M. W. (2015). Network performance comparison of VPN protocols on wired and wireless network, in *Proceeding of 2015 International Conference on Computer Communication and Informatics (ICCCI)*, 2015. Paper 978-1-4799-6805-3/15, 419-425

[10] Niu, Y., Wu, L., Wang, L., Zhang, X., & Xu, J. (2011). A configurable IPsec processor for high performance in-line security network processor, in *Proceeding of 2011 Seventh International Conference on Computational Intelligence and Security*, 2011. Paper 978-0-7695-4584-4/11, 674-678

[11] Rao, M., Newe, T., Grout, I., Lewis, E., & Mathur, A. (2015). FPGA based Reconfigurable IPSec AH core suitable for IoT applications,in *Proceeding of 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, 2015, paper 978-1-5090-0154-5/15, 2212-2216

[12] Raza, S., Duquennoy, S., Voigt, T., & Roedig, U. (2011). Demo abstract: Securing communication in 6LoWPAN with compressed IPsec, in *Proceeding of 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, ISBN 1457705133

[13] Santos, O., & Stuppi, J. (2015). *CCNA Security 210-260 Official Cert Guide*: Cisco Press. ISBN-13: 978-1-58720-566-8

[14] Shrivastava, A., & Rizvi, M. (2014). Analysis and Comparison of Major Mechanisms implementing Virtual Private Networks. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 3*(7), 2374-2381.

[15] Shue, C., Shin, Y., Gupta, M., & Choi, J. Y. (2005). Analysis of IPSec Overheads for VPN Servers, in *Proceeding of the 1st IEEE ICNP Workshop on Secure Network Protocols, (NPSec)*, 2005, paper 0-7803-9427-5/05, 25-30

[16] Shue, C. A., Gupta, M., & Myers, S. A. (2007). Ipsec: Performance Analysis and Enhancements, in *Proceeding of 2007 IEEE International Conference on Communications, ICC'07*, 2007, ISBN 1424403537, 1527-1532

[17] Singh, A. K., Samaddar, S. G., & Misra, A. K. (2012). Enhancing VPN Security through Security Policy

Management in *Proceeding of the 1st International Conference on Recent Advances in Information Technology (RAIT),* 2012, paper 978-1-4577-0697-4/12, 137-142

[18] Smaoui, S., Zarai, F., & Kamoun, L. (2012). IPSec Tunnel Establishment for 3GPP-WLAN Interworking *i*n *Proceeding of 2012 8th International Conference on Informatics and Systems (INFOS)*, 2012. ISBN9774035062, NW74-NW80

[19] Wu, J. (2009). Implementation of Virtual Private Network Based on IPSec Protocol, in *Proceeding of 2009 ETP International Conference on Future Computer and Communication*, 2009. ISBN 076953676X, 138-141

[20] Yasinovskyy, R., Wijesinha, A., & Karne, R. (2009). Impact of IPsec and 6to4 on VoIP Quality over IPv6, in *Proceeding of 2009 10th International Conference on Telecommunications,* 2009. ISBN 9531841306, 235-242