Performance Evaluation of Authenticate (MD5, SHA) Routing Traffic over EIGRP and OSPF with IPV6

Garima Jain
Department of Computer Science & Engineering
CTAE, Udaipur, India

Teena Hadpawat
Department of Computer Science & Engineering
CTAE, Udaipur, India

Dipesh Vaya
Department of Computer Science & Engineering
SSCE, Udaipur, India

ABSTRACT
A process of forwarding data on a route from source to destination is termed as routing. This process of routing data from source node to destination node is accomplished by using its protocol. Routing protocols have the responsibility of movement of data through optimal path. As routing protocol play a vital role in infrastructure of computer network, more emphasis is given to routing protocols with security constraints. EIGRP is a distance vector routing protocol which is based on DUAL (Diffusing Update Algorithm), OSPF is an interior Dijkstra algorithm based protocol. OSPF is a link state interior gateway protocol. In first, proposed network topology has been configured with EIGRP and OSPF protocols with IPV6.Then routers are authenticated using MD5 and SHA algorithms. Performance is evaluated in terms of jitter and delay time. Average delay time and average jitter time are calculated for OSPF MD5, OSPF SHA, EIGRP MD5 and EIGRP SHA. It is observe that average delay time and average jitter time for OSPF MD5 is less then EIGRP MD5 and average delay time and average jitter time for OSPF SHA is less then EIGRP SHA.

Keywords
MD5, SHA, OSPF, EIGRP, Jitter.

1. INTRODUCTION
Internet plays a vital role in the communication over network. Data is transmitted over network using a protocol called routing protocol. Routing protocol is a set of rules that is used to route data from source node to destination node. Sending data packet over network is not sufficient. Security of data is also very important, unsecured data can be or intercepted. This can lead to violation of security constraints. So it is required that data which is routed using routing protocol must be secured using security features. Routing Information Protocol (RIP), Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) are some of the routing protocols. OSPF is mostly in big business companies. Enhanced Interior Gateway Routing Protocol (EIGRP) is based on IGRP. EIGRP is a distance vector routing protocol. Routing protocols are can be attacked, that can harm individual user or the complete network operator. Attacker can interrupt the data as well as manipulate the data. Both active and passive attacks are a possibility. To prevent these types of attacks proposed technology makes use of MD5 and SHA based routing traffic authentication. In this paper, performance evaluation study is performed on MD5 and SHA authenticated routing traffic with OSPF and EIGRP protocol.

The performance of each routing protocol is different from each other. Among all routing protocols, EIGRP and OSPF routing protocols are chosen for doing performance evaluation for data traffics in secured manner. The main aim of this work is to evaluate which protocol, EIGRP or OSPF with Secured manner, is most suitable to route data traffic. The related work is reviewed in Section 2. In Section 3, MD5 [1] algorithm and SHA [2] algorithm is described. In Section 4 proposed work is described. Section 5 describes the results and graphs of the proposed work. In Section 6, Conclusion and future work is described.

2. RELATED WORK
In [11], the security of routing protocols has been analyzed. They also identified various vulnerabilities as well as threats in its design. Authors proposed a set of modifications to the protocol with the modifications they were able to reduce or remove the most vulnerable threats.

In the paper [16], a framework for Resilient Internet Routing Protocols, the various research efforts to enhance the dependability of the routing infrastructure have been suffered. It is analyzed that specific faults may be effectively guarded by individual defense mechanism, but it is not possible for single fence to counter all faults.

In paper [17], Performance Analysis and Redistribution among RIPV2, EIGRP and OSPF routing protocol, the performance analysis comparison of these three routing protocols have been done. In this, the simulated network topology has 8 Cisco routers and one switch.

In the paper [15], Analysis and Comparison of MD5 and SHA-1 algorithm implementation in simple-o authenticate based security system; in this application SHA-1+ salt algorithm was implemented. The comparison of MD5 and SHA has been performed.

2.1 MD5 Authentication
As the routing path is vulnerable to attacks and these attacks can result in lots of secret data or manipulation of the confidential data. Therefore to authenticate routing path MD5 [1] algorithm can be used. MD5 algorithm is mainly useful in digital signature application. It takes a message of arbitrary length as input and produces a 128 bit message digest of the given input. In MD5 authentication, the collaborating routers must share an authentication key. This key must be manually preconfigured on each router. especially, EIGRP and OSPF routing protocols are supported with keyed MD5 cryptographic checksums to supply authentication of traffic data as well as routing updates. Each key is portrayed by key number, key string, and key identifier, which are kept regionally. For EIGRP, multiple keys that are sorted into one keychain is used for authentication. Each key is associated with a number that should be an equivalent for all the routers and never be sent over the wire. every router uses a mix of this number and also the traffic data as inputs to the MD5

algorithm to provide a message digest known as hash. EIGRP MD5 authentication ensures that routers settle for EIGRP packets only from trustworthy sources. when the MD5 authentication is designed on an interface, each EIGRP packet sent by a router over that interface is signed with an MD5 fingerprint.

Processing Re-write Suggestions Done (Unique Article) MD5 [1] (Message-Digest algorithm) as a typical hash function, was introduced in 1992 by professor Ronald Rivest who had additionally proposed RSA public key encryption algorithm. This technique takes as input a message of absolute length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is conjectured that it's computationally impracticable to produce 2 messages having identical message digest, or to produce any message having a given pre specified target message digest. The MD5 algorithm is meant for digital signature applications, where an oversized file must be "compressed" in a secure manner before being encrypted with a non-public (secret) key beneath a public-key cryptosystem like RSA. Usually speaking, MD5 algorithm initial deals with message through dividing them into completely different blocks consistent with each 512 bit that are processed individually. Then every tiny block is divided into sixteen groups, which length is thirty two bit. Once a series of processing, the output, consists of 4 completely different teams, generates a 128 bit hash values. MD5 algorithmic rule method is shown within the Fig.1.

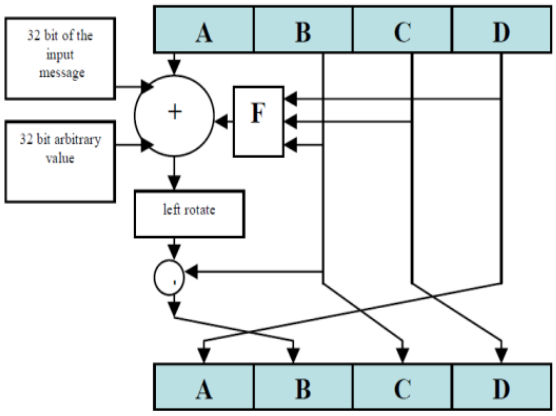

Fig 1: Process of MD5 Algorithm

In fig. 1, F is a nonlinear function of (B, C, and D).

3. PROPOSED WORK

It is intended to use available simulators (GNS3) to evaluate the performance of EIGRP and OSPF routing with different Security constraints.

Our network model consists of four Cisco 3725 modular access routers with attached terminals. A terminal connected to ROUTER5 (R5) will be used to plug directed traffic into the network. This terminal will be called the Client. While, the terminal connected to ROUTER6 is the targeted recipient of the traffic plugged by the Client, this terminal will be called the Server. The communication of traffic is implemented using a Java client/server program running on terminals attached to the designated routers. Both the Client and the Server are connected to their associated routers through their Ethernet ports. All ports for the ROUTER6 are connected via their Fast Ethernet interface. The clock rate of each router is set to 800,000Hz. Figure 4 shows the detailed configurations of the network model. Each interface assign ipv4 and ipv6 addresses. The configuration instructions of the routing protocols on the routers can be found in. The hardware clock of individual routers initially was not synchronized. To overcome this problem, it is figured ROUTER6 to host Server Network Time Protocol (SNTP).The remaining routers are configured to adjust their times based on the SNTP on ROUTER6. Routers are configured to host SNTP, namely ROUTER1, using the following commands:

sntp server 192.168.1.2

sntp broadcast client

Following commands are executed on the remaining routers:

ntp clock-period 3

ntp server 192.168.1.2

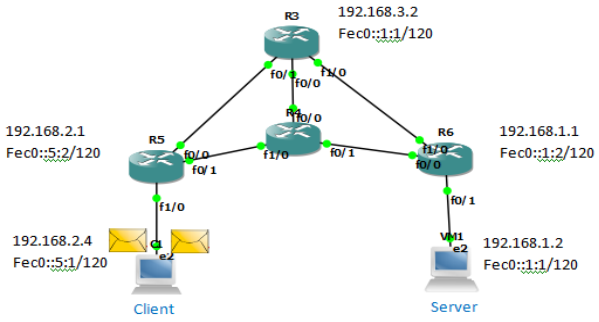

Fig.2 Routing Scenerio

3.1 A. Configure router with EIGRP IPV6

enable

Router> enable

// Enables privileged EXEC mode.

configure terminal

Router# configure terminal

// Enters global configuration mode

ipv6 unicast-routing

Router(config)# ipv6 unicast-routing

//Enables the forwarding of IPv6 unicast datagrams.

interface type number

Router(config)# interface FastEthernet 0/0

// Specifies the interface on which EIGRP is to be configured.

no shut

// Enables no shut mode so the routing process can start running.

Router(config-if)# no shut

ipv6 enable

// Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.

Router(config-if)# ipv6 enable

ipv6Eigrp 1

// Enables EIGRP for IPv6 on a specified interface.

ipv6 router eigrp as-number

Router(config-if)# ipv6 router eigrp 1

router-idip-address

Router(config-router)# router-id 1.1.1.1

exit

Router(config-router)# exit

3.2 B. Enable MD5 Authentication with EIGRP

enable

configure terminal

interface type number

no shut

ipv6 authentication mode eigrp as-number md5

// Specifies the type of authentication used in EIGRP for IPv6 packets.

ipv6 authentication key-chain eigrp as-number key-chain

// Enables authentication of EIGRP for IPv6 packets.

exit

key chain name-of-chain

// Identifies a group of authentication keys.

key key-id

// Identifies an authentication key on a key chain.

key-string text

// Specifies the authentication string for a key.

accept-lifetime start-time infinite | end-time| duration seconds

// Sets the time period during which the authentication key on key chain is received as valid.

send-lifetime start-time infinite | end-time | duration seconds

// Sets the time period during which an authentication key on a key chain is valid to be sent.

3.3 C. Enable SHA Authentication with EIGRP IPV6

enable

configure terminal

interface {default | interface-type interface-number}

authentication mode {hmac-sha-256 encryption-type password | md5}

end

3.4 *Enable MD5/SHA Authentication with OSPF IPV6*

enable

configure terminal

interface type number

Do one of the following:

// Specifies the authentication type for an

interface.

ospfv3 authentication {ipsecspi} {md5 | sha1} key-encryption-type key} |

null

ipv6ospf authentication ipsecspispi md5 key-encryption-type {key | null}end

Table 1. Table captions should be placed above the table

4. EXPERIMENTAL RESULTS

In this research, four graphs were plotted to evaluate the average delay time in sec and average jitter in ms with respect to the transmitted mean file size in KB for the two routing protocols. Various text traffic file, sent during the sessions of the ON periods, have been plugged into the simulation model. Initially, 20KB file size is loaded into the system. After Fixed time Interval all the remaining files has been sent one after the other. Figure 3 shows the average delay time with file size in the secured MD5 case of EIGRP, and OSPF routing protocols. The results show that when the system is lightly loaded, all routing protocols give almost the same average delay values with small difference. Particularly, the OSPF protocol keeps the minimum values throughout the simulation benefiting from its link state routing properties in reducing packet processing time.

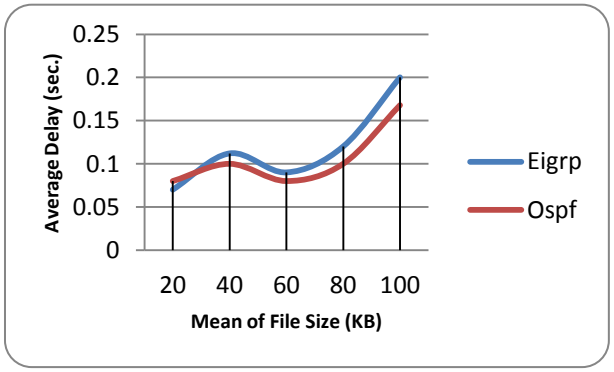

Fig. 3 Average delay time in MD5 secured case

Figure 4 shows the average delay time with file size in the secured SHA [2] case of EIGRP [7], and OSPF [9] routing protocols. The results show that when the system is lightly loaded, all routing protocols give almost the same average delay values with small difference. Particularly, the OSPF protocol keeps the minimum values throughout the simulation benefiting from its link state routing properties in reducing packet processing time.

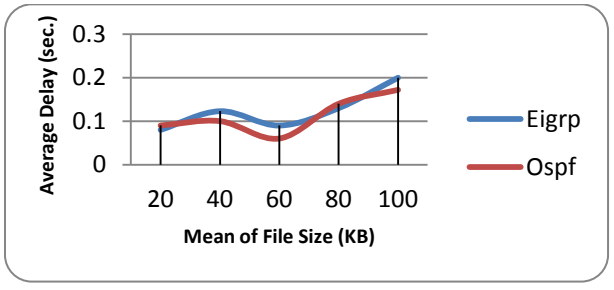

Fig. 4. Average delay time in SHA secured case.

Figure 5 shows the average jitter with file size in the secured case MD5 [1] of EIGRP and OSPF routing protocols. The results show that in the case of lightly loaded conditions, the OSPF [9] routing protocol records a remarkable minimum average delay when compared with EIGRP [7] due to its link state properties. However, starting the moderately loaded

conditions and onwards the two routing protocols preserve the same jitter values in inversely proportional fashion with respect to the file size.

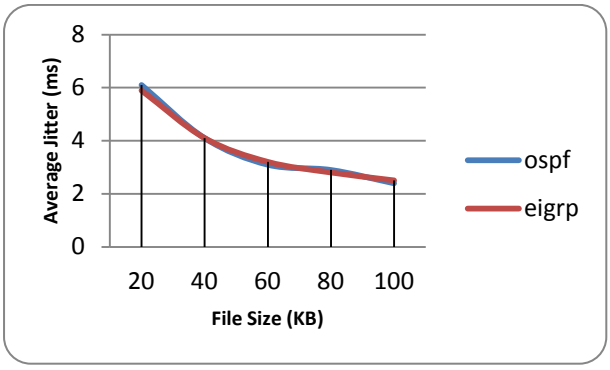

Fig. 5 Average jitter time in MD5 secured case

Figure 6 shows the average jitter with file size in the secured SHA case of EIGRP and OSPF routing protocols. The results show that Throughout the whole experiment, the two routing protocols almost show the same results with very small variation. In general, OSPF protocols lead to higher performance in both secured cases when compared to the EIGRP.

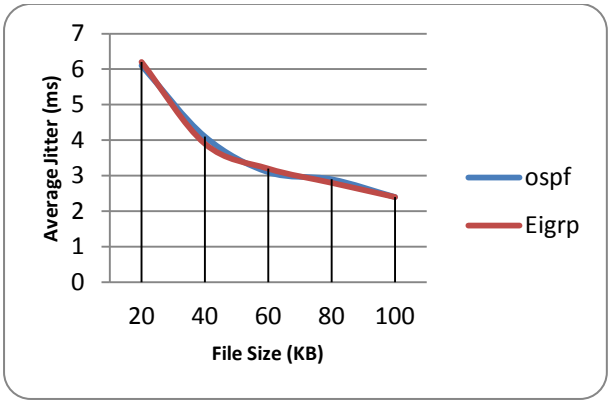

Fig. 6 Average jitter time in SHA secured case

It can also be concluded that link state routing protocols, represented by OSPF [9], are always better performed than distance vector routing protocols EIGRP [7]. This is due to the fact that link state routing is aperiodic routing scheme as opposite to the distance vector routing which is periodic.

The feature of being aperiodic routing reduces bandwidth consumption and leads for higher throughput with minimum end-to-end average delay.

5. REFERENCES

[1] Rivest, R. The MD5 Message digest algorithm, Request for commentsv(RFC) 1321, Internet Activities Board, Internet Privacy Task Force, Apr.v1992.

[2] FIPS PUB 180-1, Secure Hash Standard (SHA-1),National Institute of Standards and Technology (NIST),1995.

[3] Graziani,R. and Jonson,A. Routing protocols and concepts: CCNA exploration companion guide.Pearson Education. London,2008.

[4] Haijun1,Z., Jin1, Pan and Pubing1,S. Cost adaptive OSPF Source: Proceedings. Fifth International Conference on Computational Intelligence and Multimedia Applications. ICCIMA 2003, 55-60, 2003.

[5] Online source. (2004, Aug 27),Advanced IP Addressing Management, Cisco Systems. http://www.informit.com/articles/

[6] Cisco, IP Routing, Introduction to EIGRP, Document ID: 13669.

[7] http://www.cisco.com/en/US/tech/tk365/technology_tech_note09186a0080093f07.shtml

[8] Feldmeier, B. and Atkinson, R., OSPF MD5 Authentication, Draft ofietf-ospf-md5-02,"Naval Research Laboratory, pp. 11-11, 1994.

[9] Javvin network management and security. IS-IS: Intermediate System to Intermediate system routing protocol. http://www.javvin.com/protocolOSPF.html.

[10] Lammle, T. Cisco Certified Network Associate, 5th edition, 2005

[11] Huitema,C. Routing in the internet,2. Ed. Prentice Hall PTR, cop. 2000.

[12] http://www.cisco.com/en/US/tech/tk365/technologies_white_paper09186a0080094e9e.shtml

[13] Merike K., Designing Network Security, CiscoPress, 2003.

[14] Rivest, R., The MD5 Message-Digest Algorithm, IETF RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, 1992.

[15] Ratna,A.,Purnamasari,P.,Shaugi,A.and Salman, M.Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system.

[16] Pei, D.,Zhang,L.and Massey, D.A framework for resilient Internet routing protocols.Year,2004, Volume 18, Issue 2,Pages 5 - 12.

[17] Dey, G.,Ahmed, M., and Ahmmed K.Performance analysis and redistribution among RIPv2, EIGRP & OSPF Routing Protocol,2015. International Conference on Computer and Information Engineering (ICCIE),Year 2015, Pages 21 – 24.