IOP Conf. Series: Materials Science and Engineering **263** (2017) 042014 doi:10.1088/1757-899X/263/4/042014

Analysis of MD5 authentication in various routing protocols using simulation tools

Dinakaran M, Darshan K N and Harsh Patel

School of Information Technology and Engineering, VIT University, Vellore-632014, Tamil Nadu, India.

E-mail: dinkaran.m@vit.ac.in

Abstract. Authentication being an important paradigm of security and Computer Networks require secure paths to make the flow of the data even more secure through some security protocols. So MD-5(Message Digest 5) helps in providing data integrity to the data being sent through it and authentication to the network devices. This paper gives a brief introduction to the MD-5, simulation of the networks by including MD-5 authentication using various routing protocols like OSPF, EIGRP and RIPv2. GNS3 is being used to simulate the scenarios. Analysis of the MD-5 authentication is done in the later sections of the paper.

1. Introduction

Ronald Rivest is a well-known cryptographer who has proposed various cryptographic algorithms like RSA, RC2, and RC3 etc. has also proposed MD-4 and MD-5. MD-5 is a hash function which takes input of variable length messages and gives output of 128 bit "message digest" of the input.

MD-5 algorithm can be used for login authentication in which encryption of password takes place. Encrypted password value is compared with the password being stored in the database for authentication during login process. If the matching of the encrypted password and the password in the database is correct, then authentication is success or else authentication is failed. Figure 1 shows the MD-5 algorithm process.

GNS-3 is a graphical network simulator which helps in running simulations on the user designed network topologies. IOS routers, ATM or Frame Relay or Ethernet switches and PIX firewalls are supported in GNS3.GNS-3 helps in authenticating the path being taken by the data in the network topology by using MD-5 hash algorithm. By default, MD-5 authentication will be disabled but commands can be used to enable the MD-5 feature so that authentication happens.

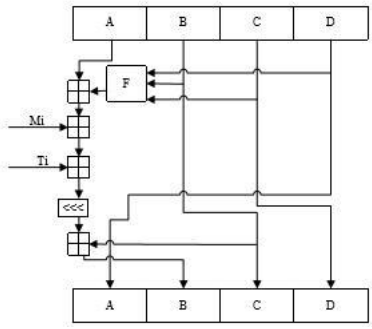

Figure 1. MD-5 algorithm process [1].

2. Literature Survey

Linxia Zhong et al [1] have proposed an improved MD5 which can resist brute force attack and differential attacks. Improved MD5 encryption algorithm helps in protecting the password information of the user's which is proved in the experiments done by the authors. Figure 2 gives the algorithm proposed by Linxia Zhong et al.

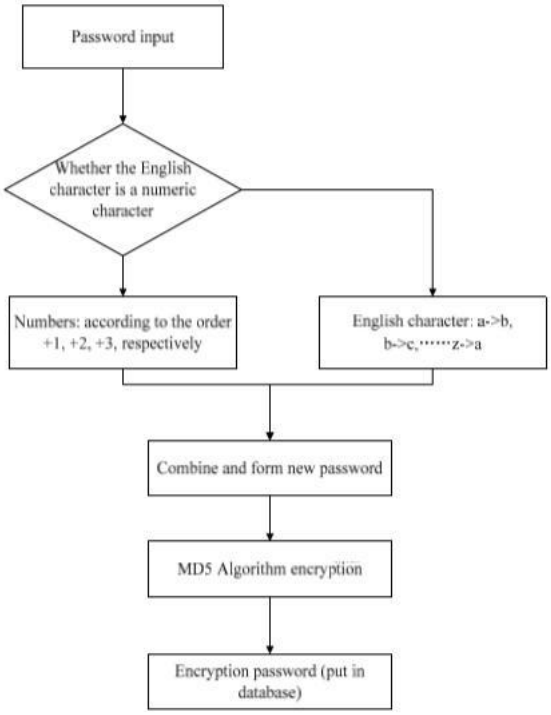

Figure 2. Improved MD-5 algorithm [1].

Improved MD-5 helps in providing the authentication and the speed at which the encryption process happens is quiet fast also.Miss Manorama Chauhan [2] has proposed a new cryptographic algorithm using MD-5 hash algorithm along with Elliptic Curve Cryptographic (ECC) encryption-decryption process. It helps in securing file transfers on all devices since it is lighter and consumes less memory and power. Evaluation of the proposed algorithm is shown by comparing the memory and time being consumed by the algorithm. Figure 3 shows the algorithm.

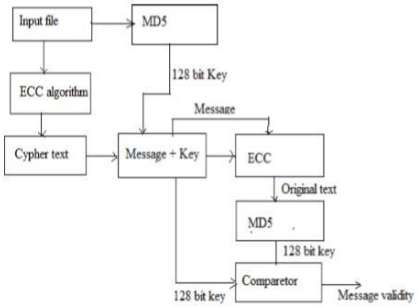

Figure 3.Improved ECC algorithm [2].

Bhale Pradeepkumar Gajendra et al [3] have proposed Identity-Based Encryption (IBE) process using both RSA and MD-5. This process helps in improving the data transmission process by providing high security as well. Hybrid algorithm proposed provides high security in cloud architecture environments. Figure 4 gives the proposed algorithm.

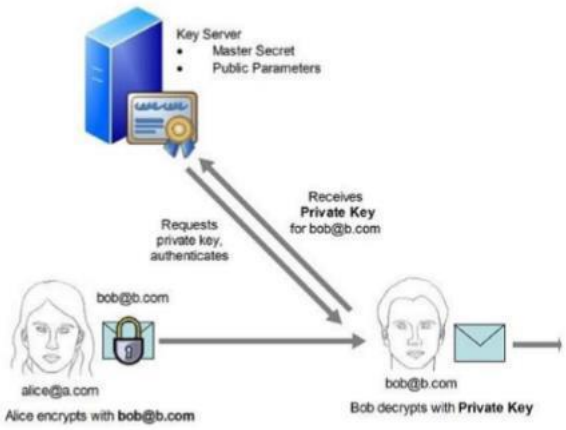

Figure 4. Identity-Based Encryption [3].

Golap Kanti Dey et al [4] have done the performance analysis and comparison of three dynamic routing protocols (RIP, EIGRP, OSPF) and redistribution as well. Switches and routers of Cisco are being used for simulation. Figure 5 shows the topology used for the simulation. Redistribution commands are being used in the middle switch which helps communicating between the different networks running different protocols.

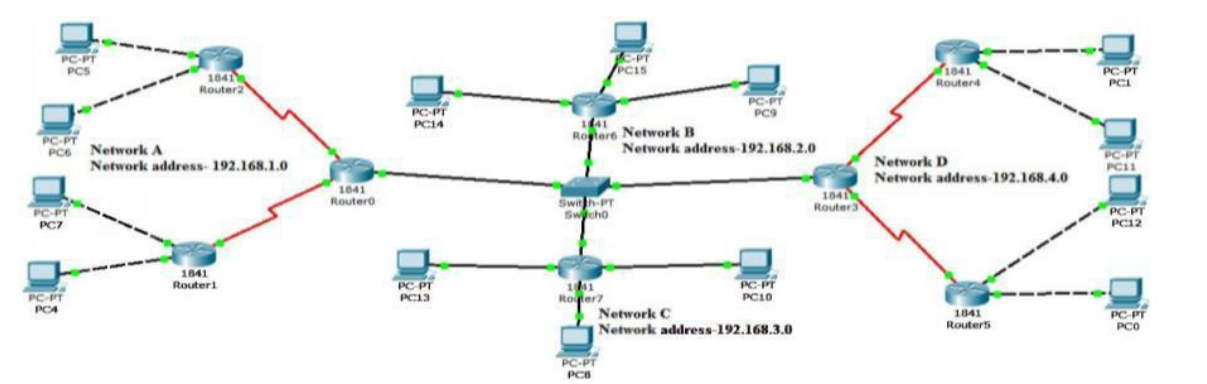

Figure 5. Simulated topology [4].

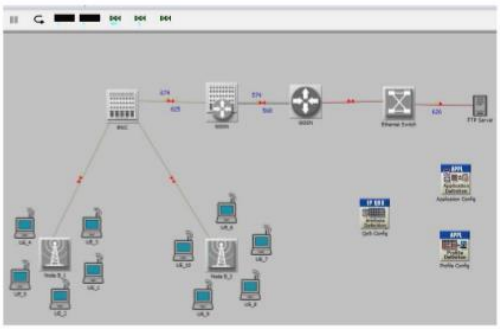

Figure 6. Topology used for simulation [5].

Meenakshi et al [5] have analysed the performance of 3G wireless technologies under the EIGRP, IGRP, RIP routing protocols. OPNET simulation tool is being used. Above Figure 6 shows the topology used by the Meenakshi et al. RIP is best with less complexity, less memory, maximum time efficiency but has less scalability. EIGRP has overall best protocol with least cost of transmission and with less queuing delay.

Khalid Abu Al-Saud et al [6] have done comparison between routing protocols like EIGRP, RIPv2 and OSPF considering different parameters like delay and jitter on devices like Cisco routers by enabling and disabling MD-5 authentication. Figure 7 gives the network model being used. Results of the experiment shows that OSPF provides best performance when compared to other protocols with less average delay and jitter.

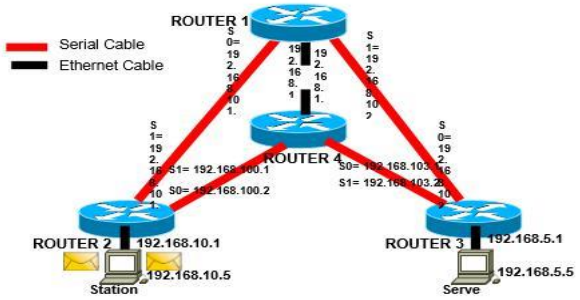

Figure 7.Proposed network topology [6].

Archana C [7] have done a comprehensive comparison between routing protocols. OSPF, EIGRP and RIPv2 are the protocols being compared. Cisco packet tracer tool is used for simulation. Figure 8 shows the topology used for the simulation in Cisco packet tracer.

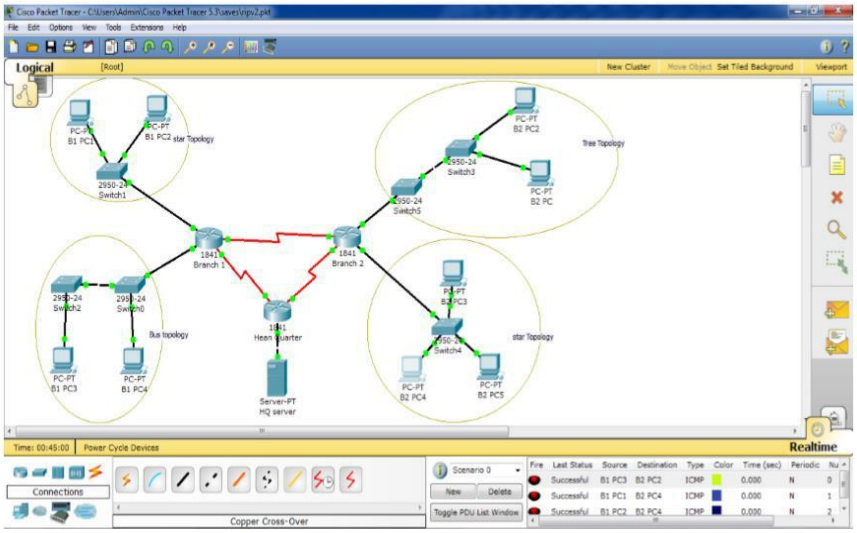

Figure 8.Network topology for simulation [7].

Khalid Abu Al-Saud et al [8] have done the evaluation of routing protocols with MD-5 authentication measures different parameters like jitter, delay time and overhead. Experiment used the scenario given in figure 9. Final results shows that the protocols without using MD-5 authentication has less delay and jitter when compared to the ones which have MD-5 authentication enabled in it.

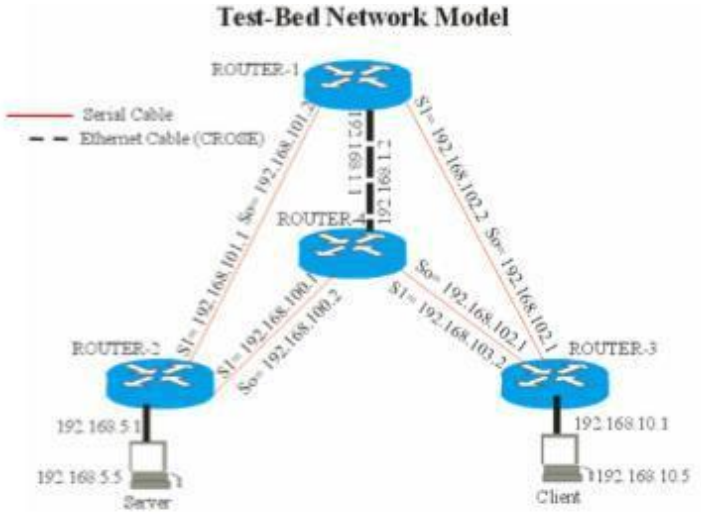

Figure 9.Test-Bed Network Model [8].

EkoSediyono et al [9] have used MD-5 along with One Time Password (OTP) and SMS gateway in order to provide high security for accessing academic information system. Algorithm uses MD-5 hash function for encrypting the OTP being generated for logging into the information system. Figure 10 shows the complete flow chart of the login system using OTP.

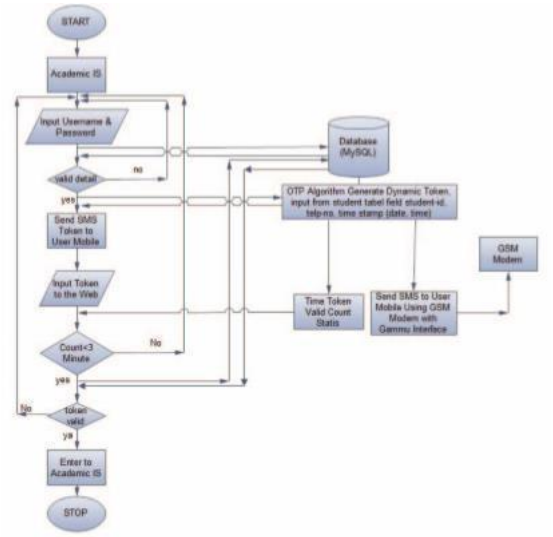

Figure 10.Flowchart of security login using OTP [9].

Chandra Wijaya [10] has done comparison of routing protocols in IPv4 and IPv6 networks using simulation. Figure 11 and figure 12 shows the IPv4 and IPv6 networks used in the simulation. Size of the packets and packet loss is smaller in EIGRP when compared to OSPF irrespective of IPv4 network or IPv6 network.

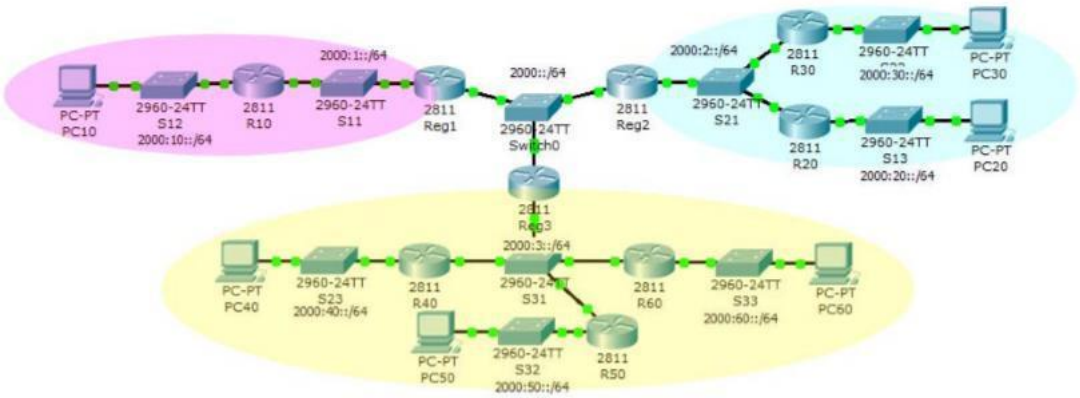

Figure 11.IPv4 Network [10].

3. Implementation

This section explains regarding the topologies being used, configuration of the nodes in the topology with commands in GNS-3.Figure 12 shows the topology used for simulation.

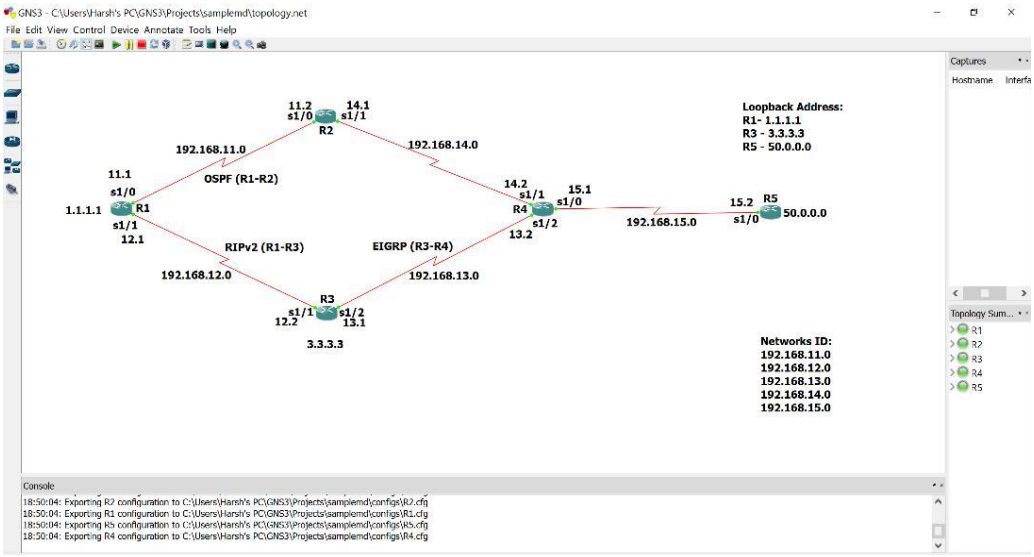

Figure 12.Network Topology.

R1, R2, R3, R4 and R5 are the cisco routers of model 3640 provided by Cisco's GNS-3. Ethernet links are used to make the connection between them as shown in figure 12. Protocols used are RIPv2, OSPF and EIGRP between routers R1 and R3, R1 and R2 and R3 and R4 respectively.

Commands used for the configuration of routers (R1 is given below) is as follows:

#Configure terminal
#Interface serial 1/0

#Ip address 192.168.11.0 255.255.255.0

#Exit

#Interface loopback 0

#Ip address 1.1.1.1 255.255.255.255

#No shutdown

#End

Commands used for configuring routing protocol OSPF with MD-5 authentication in router

R1 is as follows:

#Configure terminal

#Interface serial 1/0

#Ip address 192.168.11.1 255.255.255.0

#Ip OSPF authentication-key cisco

#Ip OSPF message-digest-key 1 MD5 cisco

#Exit

#Router OSPF 1

#Log-adjacency-changes

#Network 192.168.11.0 0.0.0.255 area 0

#Area 0 authentication

#End

#Router OSPF 1

#Network 192.168.11.0 0.0.0.255 area 0

#Area 0 authentication message-digest (command for enabling MD-5)

Commands used for configuring routing protocol EIGRP with MD-5 authentication in routerR3 is as follows:

#Configure terminal
#Router EIGRP 10 (Autonomous system number)

#Network 192.168.13.0

#No auto-summary

#Passive-interface s1/2

#Exit

#Interface loopback 0

#Ip address 3.3.3.3 255.255.255.255

#End
#Configure terminal

#Key chain root1

#Key 999

#Key-string text1

#Exit

#Exit

#Interface s1/2

#Ip authentication mode EIGRP 10 MD5

#Ip authentication key-chain EIGRP 10 root1

#End

Commands used for configuring routing protocol RIPv2 with MD-5 authentication in router

R1 is as follows:

#Configure terminal

#Interface loopback 0

#Ip address 1.1.1.1 255.255.255.255

#Interface s1/1

#Ip address 192.168.12.0 255.255.255.0

#No shut

#End

#Configure terminal

#Router RIP

#No auto-summary

#Version 2

#Network 1.0.0.0

#Network 12.0.0.0

#End

#Configure terminal

#Key-chain RIP

#Key 1

#Key-string hiHDcomputerworld

#End

#Configure terminal

#Interface s1/1

#Ip RIP authentication key-chain RIP

#End

#Configure terminal

#Interface s1/1

#Ip RIP authentication mode md5

#End

4. MD-5 Authentication

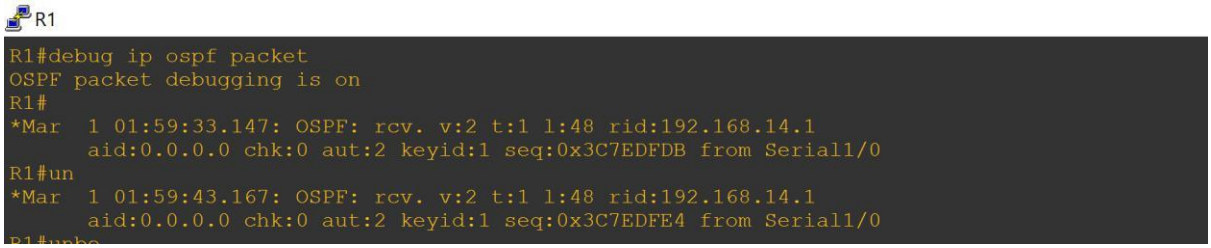

Figure 13.OSPF Authentication.

#debug ipospf packet command from router R1 will start debugging, so routers which are being MD-5 authenticated will only respond to the Hello packet sent from router R1. In this topology, router R2 will only respond to the Hello packet sent from router R1. Figure 13 shows the debug command used in router R1.

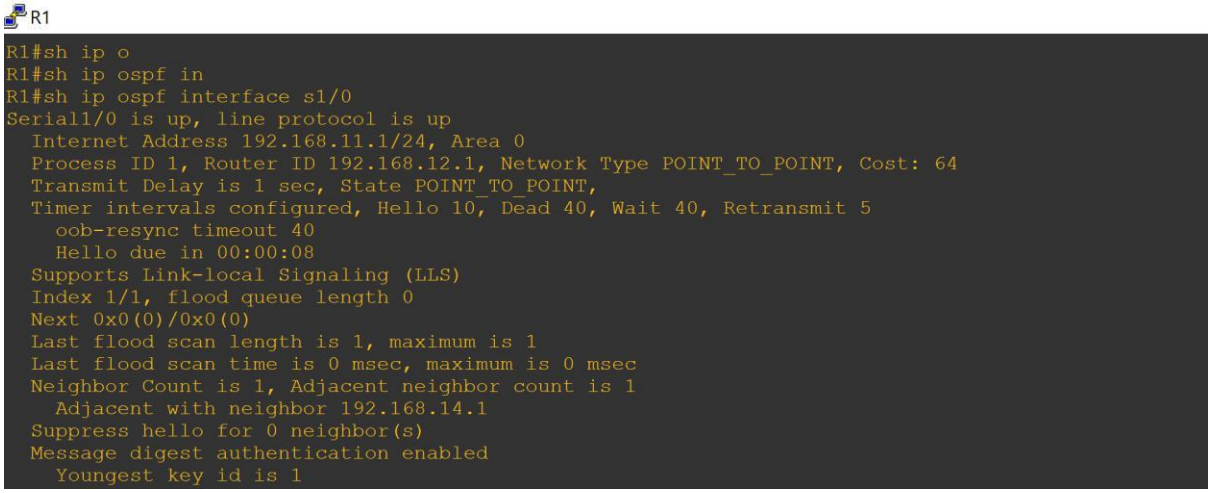

Figure 14.OSPF Authentication.

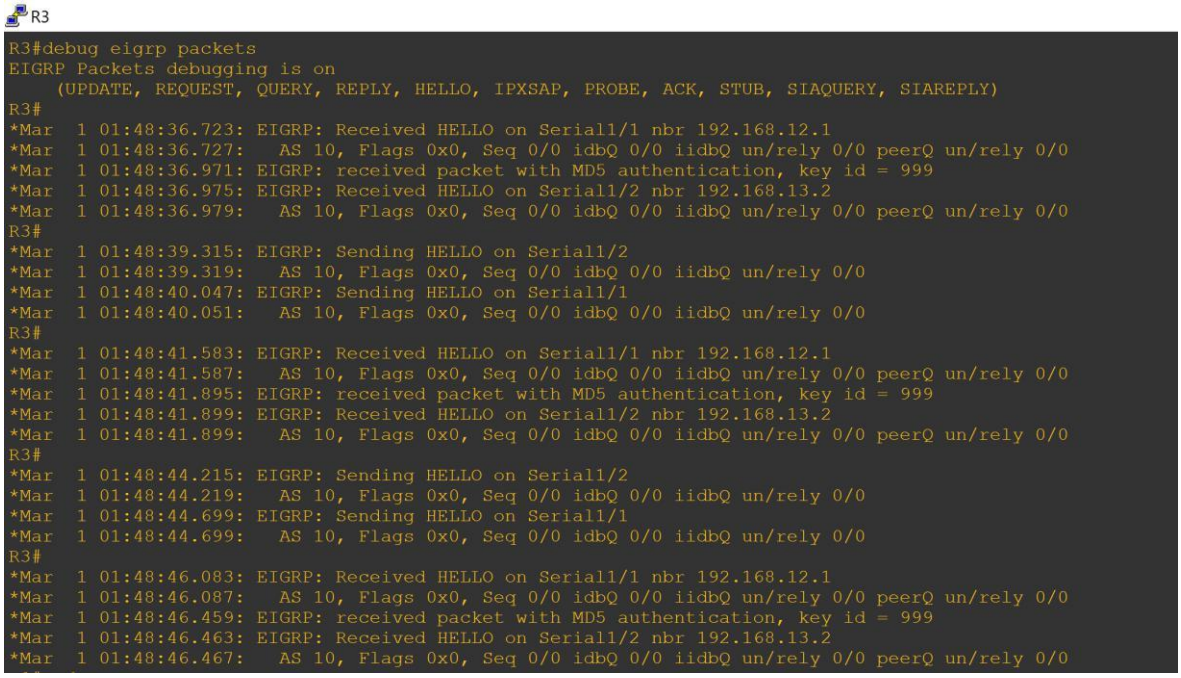

Figure 15.EIGRP Authentication.

Figure 15 shows the authentication done in the router R4 which runs EIGRP protocol between the interface of routers R4 and R3. Debug command from R4 will send Hello packet to each and every node available in the topology. But only those nodes which are being MD-5 authenticated will be able to receive those packets.

Router R3 sends the Hello packet to router R1 and router R4, but router R4 receives the Hello packets with MD-5 authentication and the key-id will be 999.

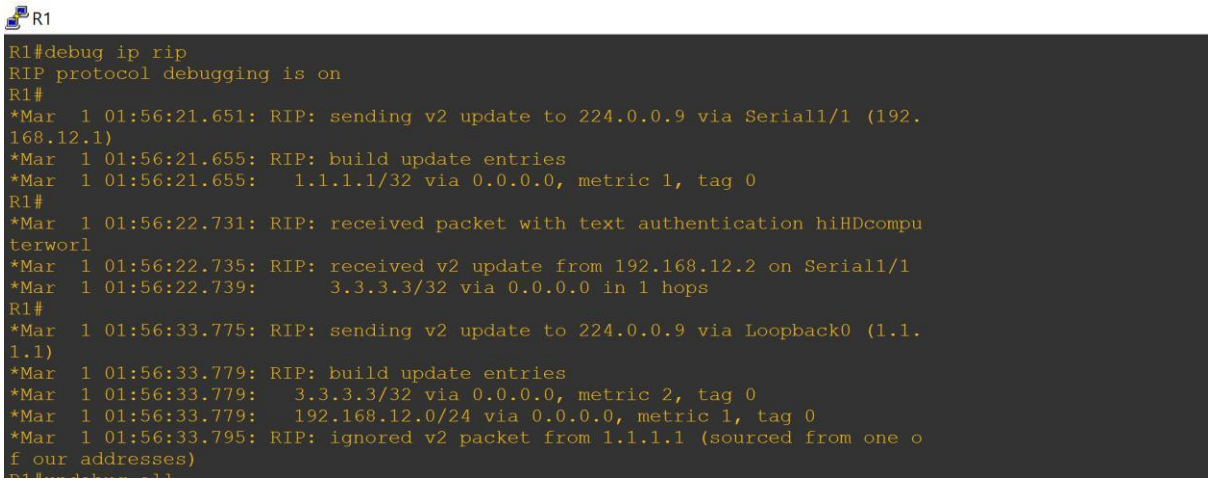

Figure 16. RIP Authentication.

Figure 16 shows the authentication between the routers R1 and R3 which runs RIPv2 routing protocol in it. Debug command is run in the router R1, router R3 actually replies back to R1, which updates its routing table.

R1

```
R1#deb
R1#debug ip
R1#debug ip r
R1#debug ip ri
R1#debug ip rip
RIP protocol debugging is on
R1#
*Mar  1 00:32:34.867: RIP: received packet with MD5 authentication
*Mar  1 00:32:34.867: RIP: received v2 update from 192.168.12.2 on Serial1/1
*Mar  1 00:32:34.871:      3.3.3.3/32 via 0.0.0.0 in 1 hops
R1#
*Mar  1 00:32:42.867: RIP: sending v2 update to 224.0.0.9 via Loopback0 (1.1.
1.1)
*Mar  1 00:32:42.871: RIP: build update entries
*Mar  1 00:32:42.871:   3.3.3.3/32 via 0.0.0.0, metric 2, tag 0
*Mar  1 00:32:42.875:   192.168.12.0/24 via 0.0.0.0, metric 1, tag 0
*Mar  1 00:32:42.883: RIP: ignored v2 packet from 1.1.1.1 (sourced from one o
f our addresses)
R1#un
*Mar  1 00:32:45.887: RIP: sending v2 update to 224.0.0.9 via Serial1/1 (192.
168.12.1)
*Mar  1 00:32:45.891: RIP: build update entries
*Mar  1 00:32:45.891:   1.1.1.1/32 via 0.0.0.0, metric 1, tag 0
```

Figure 17. RIP Authentication.

Figure 17 shows the updating of routing table of router R1 upon receiving Update message from router R3.

5. Conclusion

MD-5 hash function helps in authenticating the routers. RIPv2, EIGRP and OSPF routing protocols supports MD-5 authentication. This paper has shown the implementation of MD-5 in routers with different protocols between the interfaces. Using this kind of authentication may lead to certain amount of delay, but security is more important for certain applications rather than delay, but delay sensitive applications can avoid authentication.

Ronald Rivest is a well-known cryptographer who has proposed various cryptographic algorithms like RSA, RC2, and RC3 etc. has also proposed MD-4 and MD-5. MD-5 is a hash function which takes input of variable length messages and gives output of 128 bit “message digest” of the input.

MD-5 algorithm can be used for login authentication in which encryption of password takes place. Encrypted password value is compared with the password being stored in the database for authentication during login process. If the matching of the encrypted password and the password in the database is correct, then authentication is success or else authentication is failed. Figure 1 shows the MD-5 algorithm process.

GNS-3 is a graphical network simulator which helps in running simulations on the user designed network topologies. IOS routers, ATM or Frame Relay or Ethernet switches and PIX firewalls are supported in GNS3.GNS-3 helps in authenticating the path being taken by the data in the network topology by using MD-5 hash algorithm. By default, MD-5 authentication will be disabled but commands can be used to enable the MD-5 feature so that authentication happens.

References

[1] Linxia Zhong, Wanggen Wan and Deke Kong 2016 *IEEE* 131-13.

[2] Miss Manorama Chauhan *IEEE*
[3] Bhale Pradeepkumar Gajendra, Vinay Kumar Singh and More Sujeet 2016 *IEEE* 1304-1309
[4] Golap Kanti Dey, Md. Mobasher Ahmed and Kazi Tanvir Ahmmed 2016 *IEEE* 21-24
[5] Meenakshi, Akhil Kaushik and Satvika 2014 *IEEE* 399-403
[6] Khalid Abu Al-Saud, Hatim Tahir, Moutaz Saleh and Mohammed Saleh 2010 *IAJIT* 380-387.
[7] Archana C 2015 *IJESIT* 215-222
[8] Khalid Abu Al-Saud, Hatim Mohd Tahir, Moutaz Saleh and Mohammed Saleh 2008 *JCS* 721-728.
[9] Eko Sediyono, Kartika Imam Santoso and Suhartono 2013 *IEEE* 1604-1608
[10] Chandra Wijaya 2011 *IEEE* 355-360