Journal of Computer Science 4 (9): 721-728, 2008
ISSN 1549-3636

Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 and OSPF

[1, 2]Khalid Abu Al-Saud, [2]Hatim Mohd Tahir, [1]Moutaz Saleh and [1]Mohammed Saleh
[1]Department of Computer Science and Engineering College of Engineering,
Qatar University P.O. Box 2713 Doha, Qatar
[2]Department of Computer Science Faculty of Information Technology,
University Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia

Abstract: Problem Statement: With the free flow of routing data and the high availability of computer resources, possible threats to the networks can result in loss of privacy and in malicious use of information or resources that can eventually lead to large monetary losses. **Approach:** MD5 Authentication: Due to the major role that routing protocols play in computer network infrastructures, special cares has been given to routing protocols with built-in security constraints using authentication techniques, MD5 will be presented for this work. **Results:** The study evaluates the impact of the MD5 authentication on routing traffic for the case of EIGRP, RIPv2 and OSPF routing protocols in case of secured and non-secured routing traffic and measures the delay time, jitter and overhead. **Conclusions:** This study shows that the average delay time and jitter in the secured MD5 case can become significantly larger when compared to the unsecured case even in steady state conditions. Also, the EIGRP protocol shows the minimum overhead even when the system is extremely overloaded.

Keywords: Impact of MD5, EIGRP, RIPv2, OSPF, and secured routing protocols

INTRODUCTION

The past few years have witnessed an ever-growing reliance on computer networks for business transactions. With the free flow of data and the high availability of computer resources, owners and managers of enterprise networks have to secure their resources from any possible threats to their networks. Although these threats take many forms, they all result in loss of privacy to some degree and in malicious use of information or resources that can eventually lead to large monetary losses [4].

Hence, over the past few years, a number of research study have been done in routing [1,2,3]. In [1], for example, an experimental setup was developed to capture all packets crossing a router for 13 hours and give statistics about their delay characteristics. The experiment showed that in-router packet processing time accounts for a significant portion of the overall packet delay and should not be neglected. Accordingly, a solution to directly report router delay information based on busy period statistics has been proposed. Also, in[2], the authors presented an approximate model for measuring the time from which a burst transmission request is received by a source to the time at which the last packet in the burst passes through the router. The results showed that burst delay offers acceptable performance only in the blowup region obtained for router delay even for small values of router utilization. Eventually, in[3], the security of the Border Gateway Protocol (BGP) and its cost were analyzed and evaluated in terms of performance and delay. The study identified a number of threats involving the deception, disruption, and disclosure of BGP routing message traffic, and minimized most of these threats. Indeed, the authors showed that it is possible to effectively and efficiently secure the BGP routing protocol.

In this study, we will evaluate the impact of MD5 authentication of EIGRP, RIPv2 and OSPF routing traffic in two contexts: Secured and un-secured. To meet this objective, a network test-bed model of four Cisco routers has been employed. A traffic generation and analysis tools have been developed to generate traffic data and to measure the delay time, jitter and overhead as our performance measures of interest.

The remainder of the article is organized to describe the EIGRP, RIPv2 and OSPF routing protocols, presents the authentication technique used to secure the EIGRP, RIPv2 and OSPF, namely the MD5 authentication, illustrates the real model of Cisco

Corresponding Author: Khalid Abu Al-Saud, Department of Computer Science and Engineering College of Engineering, Qatar University P.O. Box 2713 Doha, Qatar

routers proposed in this work and outlines the operations and the interactions among the four routers. Finally, the article shows the results of our experimental work and the impact evaluation, before summarize our current work, and lay down the milestones for the future study.

MATERIALS AND MATHODS

EIGRP: Due to the major role of routing protocols in network infrastructures, special attentions have been given to routing protocols with built-in security functionalities[4]. The same distance vector technology found in IGRP is also used in EIGRP and the underlying distance information remains unchanged[5].

EIGRP[6] is an intra-domain routing protocol that leverages the strong points of both distance-vector and link-state protocols: it converges quickly while remaining loop free at all times. This is achieved by using a system of diffused computation where every route calculation is computed in a coordinated fashion among multiple routers. EIGRP is based on the Diffusing Update Algorithm (DUAL) which is used to compute shortest paths in a distributed manner and without ever creating routing-table loops or incurring counting-to-infinity behavior.

EIGRP's updates are similar to a distance-vector protocol, as they are vectors of distances transmitted only to directly connected neighbors. However, the updates are partial, non-periodic, and bounded. They are partial since the updates contain only the changed routes, and not the entire routing table. They are only sent whenever a metric or topology change occurs (non-periodic), and they are sent to the affected routers only (bounded). EIGRP has shown to provide loop freedom and quick convergence in medium-scale networks. To determine the path cost function of EIGRP, the formula is generally stated as:

$$C = \left(k1b + \frac{k2b}{256 - l} + k3d \right) \frac{k3}{r - k4}$$

Where:

- b = The minimum bandwidth measured in kb sec^{-1}
- l = The load on the link expressed as a number from 0- 255 (255 is 100 % loading)
- d = The total delay in unit of tens of milliseconds
- r = The reliability along the length of the path 255 for 100%.
- k1-k5 = Administrator-configurable coefficients (although the values must be consistent across the domain).

However, even this calculation is complicated by the need to scale bandwidth and delay as $b = (256 \times 10^8)/b_0$ and $d = 256d_0$, where b0 and d0 are the measured or configured values; the 256 arises from a storage difference (from IGRP to EIGRP) between 24 and 32 bits. Indeed, it is claimed that the default coefficient values of k1=1, k2 = 0, k3 = 1, k4 = 0 and k5 = 0 lead to the simplified path cost of $C = b + d$[7].

Recently, network architects state that EIGRP is being implemented in approximately half of the networks[8]. EIGRP is not only an enterprise-oriented routing protocol, but also a protocol that can be used in service-provider environments because it has fewer topology limitations than other routing protocols[9].

RIPv2: Routing Information Protocol version 2 (RIPv2) is an interior gateway protocol (IGP) created for use in small and homogeneous networks. It is a classical Distance-Vector routing protocol. RIPv2 uses broadcast User Datagram Protocol (UDP) data packets to exchange routing information. Since RIPv2 uses UDP as its delivery mechanism, the routing updates sent to the neighboring routers are not guaranteed. The sending of the RIPv2 table entries between routers defaults to 30 seconds after the initial startup of the router. This advertising of routes occurs also between two routers when a router becomes active on a connection to an already active router. RIPv2 sends the updates to the interfaces in the specified networks. If an interface's network is not specified, it will not be advertised in any RIPv2 update. The RIPv2 metric is composed of hop count, and the maximum valid metric is 15. Anything above 15 is considered infinite; we can use 16 to describe an infinite metric in RIPv2[10].

OSPF: OSPF uses link-state technology in which routers send each other information about the direct connections and links which they have to other routers. Each OSPF router maintains an identical database describing the autonomous systems topology. From this database, a routing table is calculated by constructing a shortest path tree. OSPF recalculates routes quickly in the face of topological changes, utilizing a minimum of routing protocol traffic. OSPF provides support for equal-cost multi-path. An area routing capability is also provided, enabling an additional level of routing protection and a reduction in routing protocol traffic. In addition, all OSPF routing protocol exchanges are authenticated and the OSPF metric is a cost value based on 10^8/bandwidth of the link in bits sec^{-1}. OSPF allows sets of networks to be grouped together. Such a grouping is called an area. The topology of an area is hidden from the rest of the autonomous system. This information hiding enables a significant reduction in routing traffic[11].

Authentication: The damage that can be done in an unsecured routing infrastructure is so enormous that special precautions have to be taken into consideration. Modifying routing tables maliciously can cause significant network traffic to be diverted to the wrong destination. In general, a non-secure routing infrastructure degrades the performance of routers when they are intentionally or unintentionally miss-configured. Unfortunately, no widely deployed secure routing protocols are used today. The current way of protecting routing infrastructures relies on so-called best practices, which include various simplistic techniques such as firewalls, intrusion detection systems, authentication Message Digest (MD5), route filters, and private addressing[9]. Authentication occurs when any router ensures that only routing updates received from a trusted neighbor are used. This prevents a router from accepting and using unauthorized, malicious, or corrupted routing updates that may compromise the security or availability of the network, and lead, for example, to rerouting of traffic or a denial of service[12].

The well known MD5 algorithm[13] operates on a 128-bit state, which are divided into four 32-bit blocks and denoted by A, B, C and D as shown in Fig. 1. The algorithm processes 512-bit message block in a round. Each message block modifies the MD5 state by performing 16 similar operations in a round. Each operation uses a non-linear function F, a modular addition, and a shift left rotation respectively. Figure 1 illustrates one operation.

In MD5 authentication, the participating routers must share an authentication key. This key must be manually preconfigured on each router. For EIGRP, multiple keys can be used for authentication. Each key is associated with a number, which must be the same for all the routers and never be sent over the wire. Each router uses a combination of this number and the traffic data as inputs to the MD5 algorithm to produce a message digest called hash. For RIPv2, when keyed MD5 is used, the same header and content are used, except that the 16-byte authentication key field is reused to describe a Keyed Message Digest trailer. For OSPF, the OSPF packet header includes an Authentication Type field and 64 bits of data for use by the appropriate authentication scheme. Generally, most fields within this common header have obvious meanings. For instance, the version number is set to 2 to indicate OSPFv2 and the type is the OSPF packet type i.e., hello, database description, link-state request, link-state update, and link-state acknowledgment[14].

The packet length is the number of bytes in the packet. Figure 2 illustrates the sequence of events involved in MD5 authentication for the sending router.

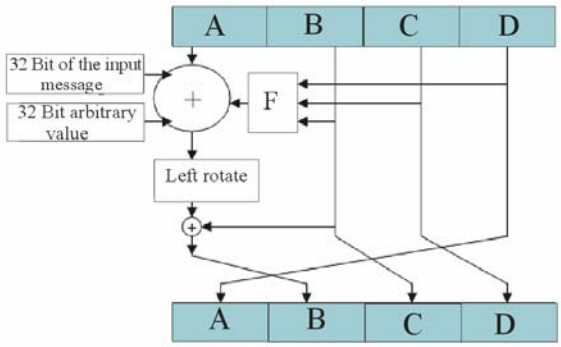

Fig. 1: MD5 Algorithm; F: is a nonlinear function of (B, C, and D)

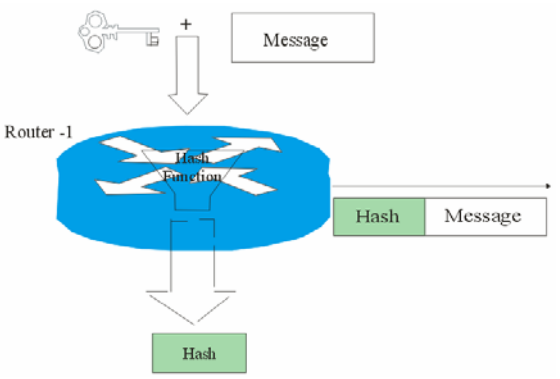

Fig. 2: MD5 Neighbor Authentication at the Sending Router

The MD5 algorithm takes the preconfigured shared secret key and the traffic data (or message) as inputs and returns a message digest (hash) that is appended to the message and sent through the appropriate interface[15]. Figure 3 illustrates the sequence of events for routing protocol authentication at the destination router. EIGRP, RIPv2 and OSPF are supported keyed MD5 cryptographic checksums to provide authentication of traffic data including routing updates. Each key is represented by key number, key string, and key identifier, which are stored locally. EIGRP MD5 authentication supports multiple keys, which are grouped in one keychain. RIPv2 MD5 the basic RIPv2 message format provides for an 8-byte header with an array of 20-byte records as its data content. When keyed MD5 is used, the same header and content are used, except that the 16-byte authentication key field is reused to describe a Keyed Message Digest trailer. With MD5, all OSPF protocol exchanges are authenticated. The OSPF packet header includes an

Authentication Type field and 64 bits of data for use by the appropriate authentication scheme. Each key has a lifetime period that validates the usage of this key for sending and receiving. The router selects one key from the keychain for sending an authentication packet. The key numbers are examined from the lowest to the highest, and the first valid key encountered is used[16,17].

The test-bed network model: We intended to use available simulators to study the impact MD5 of EIGRP, RIPv2 and OSPF routing with and without security constraints. However, an intensive survey of the available simulators e.g. Network Visualizer, Packet Tracer, and Boson, has revealed that none of these simulators support authentication commands. Therefore, present network model has been experimentally implemented in present research lab using physical Cisco 1721 routers. Our end-to-end experimental model consists of four Cisco 1721 modular access routers. A traffic generator is plugged into a randomly chosen router at one end targeting any of the remaining routers. At the targeted router, the average traffic delays, jitter and overhead are computed. This communication of traffic is implemented using a java client/server program running on terminals attached to the designated routers. Following, the experiment and simulation settings and configurations of the routers are explained in details.

The actual experiment settings and routers configurations in both secured and unsecured modes are presented here. Simulation construction includes traffic patterns used, routers time synchronization, client-server program and other issues.

Setup and configuration of the routers: The test-bed network model is shown in Fig. 4. The client is connected to ROUTER3 and the server is connected to ROUTER2 through their Ethernet ports. ROUTER1 and ROUTER4 are connected via their Ethernet using UTP cross cable. Other ports for the ROUTERS are connected via their WAN Interface Cards (WIC), namely WIC0 and WIC1. The clock rate on DCE (WIC1) terminal of each router is set to 800,000 Hz.

Without authentication, the ROUTER1 configuration is shown in Fig. 5. A major issue we faced during the setup of our model is the synchronization between the routers. The issue is that the hardware clock of individual routers is usually not synchronized. To overcome this problem, we configured one of the routers to host SNTP, namely ROUTER1, using the commands:

```
sntp server 192.168.102.2
    sntp broadcast client
```

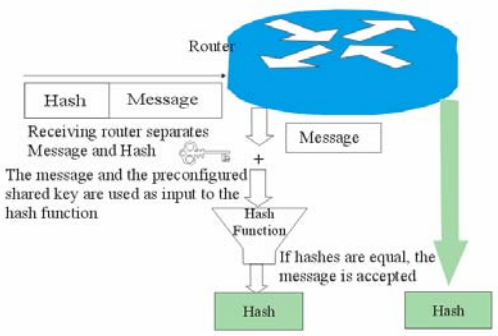

Fig. 3: The Sequence of Events at the destination router

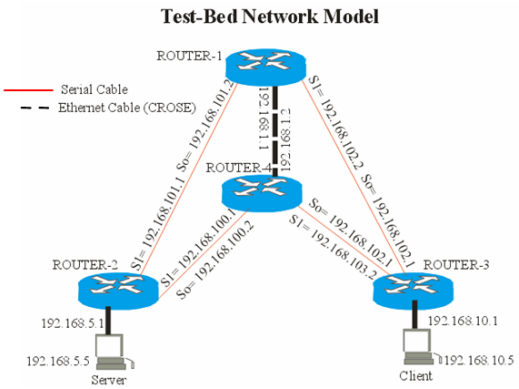

Fig. 4: The Proposed Test-Bed Network Model of Cisco Routers

The last part of the configuration shows that ROUTER1 is hosting the Server Network Time Protocol (SNTP). Other routers configuration are done in a similar way except, they will adjust their time based on the SNTP router. Therefore, we executed the following commands on the remaining routers:

```
ntp clock-period 10
ntp server 192.168.102.2
```

The IP addresses used are the same as those shown in the network model of Fig. 4. Another major issue we faced the synchronization between the end-to-end nodes. For solving this problem, we used clocksynch tool from PMSystem at the end nodes to synchronize their clocks with the whole test-bed network model.

Before enabling authentication to provide secured routing updates, a keychain and at least one key must be created. Thus, to create such keychain and key, we show our router configurations for the cases of EIGRP, RIPv2, and OSPF routing protocols in Fig. 6, Fig. 7, and Fig. 8 respectively.

```
Hostname Router1
Interface FastEthernet0
Ip address 192.168.1.1 255.255.255.0
Speed auto
Interface Serial0
Ip address 192.168.101.2 255.255.255.0
Interface Serial
Ip address 192.168.102.2 255.255.255.0
Clockrate 800000
Router eigrp 100
Network 192.168.1.0
Network 192.168.101.0
Network 192.168.102.0
Auto- Summary
Ntp master 10
Sntp server 192.168.102.2
Sntp broadcast client
```

Fig. 5: ROUTER1 Configuration in the unsecured mode

Case EIGRP: Enter global configuration mode
ROUTER1#configure terminal
Create the key chain
Router1(config)#key chain khalidchain
Specify the key number
Router1(config−keychain)#key 1
Specify the key−string for the key
Router1(config−keychain−key)#key-string khalid-63
End the configuration
Router1(config-keychain-key)#end

We then configure EIGRP to perform MD5 authentication using the key as shown:
Enter global configuration mode
Router1#configure terminal

From global configuration mode, specify the interface that you want to configure EIGRP message authentication on. In this case is Fastethernet 0
Router1(config)#interface fastethernet 0
Enable EIGRP message authentication. The 100 used here is the autonomous system number of the network. md5 indicates that the md5 hash is to be used for authentication:
Router1(config-if)#ip authentication mode eigrp 100 md5
Specify the keychain that should be used for authentication
ROUTER1(config-if)#ip authentication key-chain eigrp 100 khalidchain
ROUTER1(config-if)#end

Case RIPv2: We then configure RIP-v2 to perform MD5 authentication using the key as shown in Fig. 7.

Case OSPF: We then configure OSPF to perform MD5 authentication using the key as shown in Fig. 8.

```
ROUTER-1#sh run
Building configuration...
Version 12.4
Hostname Router-1
Key chain khalidchain
 Key 1
  Key-string khalid-63
  Accept-lifetime 00:00:00 Dec 31 2008 infinite
  Send-lifetime 00:00:00 Dec 31 2008 infinite
Interface FastEthernet0
 Ip address 192.168.1.1 255.255.255.0
 Ip authentication mode eigrp 100 md5
 Ip authentication key-chain eigrp 100 khalidchain
 Speed auto
Interface Serial0
 Ip address 192.168.101.2 255.255.255.0
 Ip authentication mode eigrp 100 md5
 Ip authentication key-chain eigrp 100 khalidchain
 Clockrate 800000
Interface Serial1
 Ip address 192.168.102.2 255.255.255.0
 Ip authentication mode eigrp 100 md5
 Ip authentication key-chain eigrp 100 khalidchain
Router EIGRP 100
 Network 192.168.1.0
 Network 192.168.101.0
 Network 192.168.102.0
 Auto-summary
Ntp master 10
Sntp server 192.168.102.2
Sntp broadcast client
```

Fig. 6: ROUTER1 Configurations EIGRP in the secured mode

```
ROUTER-1#show run
Building configuration...
Version 12.4
Hostname ROUTER-1
Key chain khalidchain
 Key 1
  Key-string khalid63
  Accept-lifetime 00:00:00 Jan 31 2008 infinite
  Send-lifetime 00:00:00 Jan 31 2008 infinite
Interface FastEthernet0
 Ip address 192.168.1.2 255.255.255.0
 Ip rip authentication mode md5
 Ip rip authentication key-chain khalidchain
 Speed auto
Interface Serial0
 Ip address 192.168.103.1 255.255.255.0
 Ip rip authentication mode md5
 Ip rip authentication key-chain khalidchain
 Clockrate 800000
Interface Serial1
 Ip address 192.168.100.1 255.255.255.0
 Ip rip authentication mode md5
 Ip rip authentication key-chain khalidchain
Router rip
 Version 2
 Network 192.168.1.0
 Network 192.168.100.0
 Network 192.168.103.0
```

Fig. 7: ROUTER1 Configurations RIPv2 in the Secured Mode

The experimental model: A Java-based Object-oriented discrete-event program with both client and server is implemented at the end nodes of the network model. The network traffic, namely TCP packets, is directed from the client to the server, which calculates the major performance measures, especially the average delay time of the TCP packets. The packet data size is set to 1000 bytes and the generation of these packets follows the Markov Modulated Poisson Process (MMPP), which is a doubly stochastic Poisson process whose rate varies according to a Markov process.

```
ROUTER-1#sh run
Building configuration...
Hostname ROUTER-1
Interface FastEthernet0
 Ip address 192.168.1.1 255.255.255.0
 Ip ospf message-digest-key 1 md5 khalid-63
 Speed auto
Interface Serial0
 Ip address 192.168.101.2 255.255.255.0
 Ip ospf message-digest-key 1 md5 khalid-63
 Clockrate 800000
Interface Serial1
 Ip address 192.168.102.2 255.255.255.0
 Ip ospf message-digest-key 1 md5 khalid-63
Router ospf 100
 Log-adjacency-changes
 Area 0 authentication message-digest
 Network 192.168.1.0 0.0.0.255 area 0
 Network 192.168.101.0 0.0.0.255 area 0
 Network 192.168.102.0 0.0.0.255 area 0
Ntp master 10
Sntp server 192.168.102.2
Sntp broadcast client
```

Fig. 8: ROUTER1 Configurations OSPF in the Secured Mode

The MMPP can be viewed as a superposition of latent Poisson processes, which can be expressed as a non-homogeneous discretely indexed Hidden Markov Model (HMM) by partitioning time into intervals between observed events. The resultant traffic model is an ON/OFF traffic where the client sends bulk traffic during the ON periods and nothing during the OFF periods. ON and OFF periods are distributed exponentially with a mean of 10. The number of packets in bulk traffic is distributed normally with mean equals to 100 and variance equals to 10.

RESULTS AND DISCUSSION

Here, five graphs were plotted to evaluate the average delay time, jitter and overhead with respect to the number of packets. Various traffic loads described by total number of packets sent during the sessions of the ON periods have been plugged into the simulation model. Initially a total of 10,000 packets as a first traffic load incremented by 5,000 packets up to 55,000 packets have been used. Figure 9 shows the average delay time with number of packets in the unsecured case of EIGRP, RIPv2, and OSPF routing protocols.

The results show the average delay time of RIPv2 is continuously larger than the other two routing protocols. However, when the system is moderately overloaded both OSPF and EIGRP gives the same results before the last one increase more when the system starts to extremely overloaded with 40000 packets processed.

Figure 10 shows the average delay time with number of packets in the secured MD5 authentication case of EIGRP, RIPv2, and OSPF routing protocols.

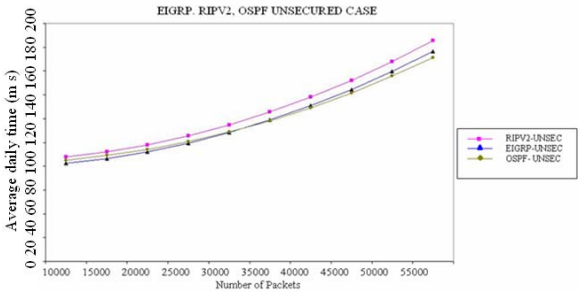

Fig. 9: Average Delay Time in Unsecured of EIGRP, RIPv2, OSPF Routing Protocols

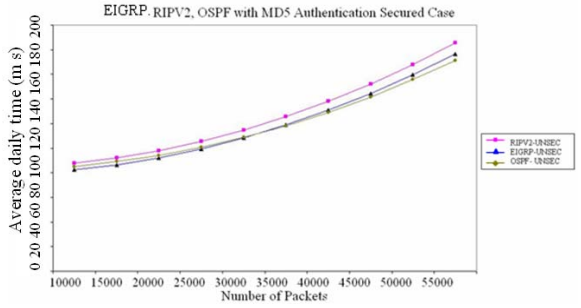

Fig. 10: Average Delay Time in Secured MD5 Authentication of EIGRP, RIPv2, OSPF

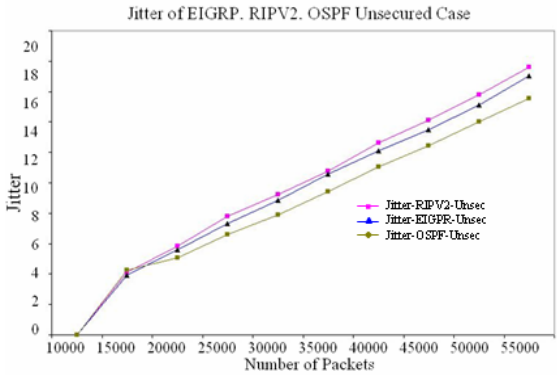

Fig. 11: Jitter in Unsecured case of EIGRP, RIPv2, and OSPF

The results show the average delay time of RIPv2 in the secured MD5 authentication case is continuously larger than the other two routing protocols. However, both EIGRP and OSPF protocols give almost the same results during the simulation. This is due to the fact that both protocols have the properties of link state which minimize the packets' processing delay time.

Figure 11 shows the jitter with number of packets in the unsecured case of EIGRP, RIPv2, and OSPF routing protocols.

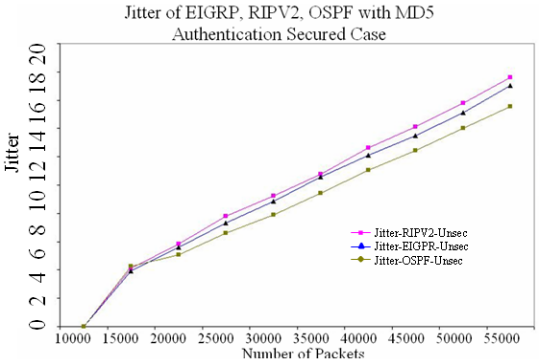

Fig. 12: Jitter in Secured MD5 authentication of EIGRP, RIPv2, OSPF

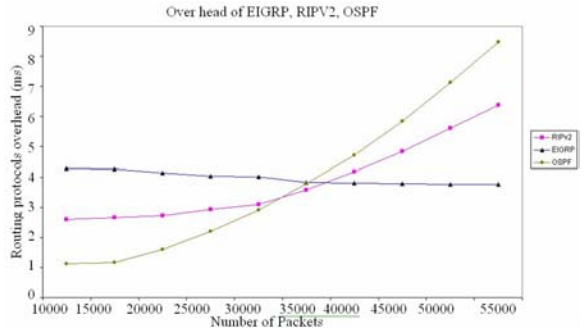

Fig. 13: Overhead of EIGRP, RIPv2, OSPF routing protocols

The results show that in the case of lightly loaded conditions, the three routing protocols preserve the same jitter value. However, when the system starts to moderately overloaded both RIPv2 and EIGRP show lager values when compared to the OSPF routing protocol. This is due to the fact that OSPF has the minimal average delay variation as shown earlier.

Figure 12 shows the jitter with number of packets in the secured MD5 authentication case of EIGRP, RIPv2, and OSPF routing protocols.

The results show that in the case of lightly loaded conditions with secured MD5 authentication case, the three routing protocols again preserve the same jitter value. However, when the system starts to moderately overloaded the RIPv2 shows lager values when compared to the EIGRP and OSPF routing protocols. This is due to the fact that both EIGRP and OSPF have the minimal average delay variation as shown earlier.

Figure 13 shows the average delay overhead of EIGRP, RIPv2, and OSPF routing protocols.

The results show that when the system is lightly overloaded OSPF gives the lowest overhead while EIGRP gives the largest one. However, when the system starts to moderately overloaded the three routing protocols give almost the same overhead with an approximate value of 3.5 ms. Eventually, when the system is extremely overloaded, both RIPv2 and OSPF show an exponentially overhead while EIGRP remains almost stable.

CONCLUSIONS

In this study, we studied the impact of secured MD5 authentication versus un-secured for EIGRP, RIPv2, and OSPF routing protocols. We first described the actual model for carrying out the experiment. A Java client-server program for generating and monitoring traffic and reporting results was presented as part of this work. The results obtained from the experiment showed that the average delay time and jitter in the secured case can become significantly larger when compared to the unsecured case even in steady state conditions. However, the EIGRP protocol shows the better performance by achieving the minimum overhead even when the system is extremely overloaded.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of Qatar University.

REFERENCES

1. Honn, N. N. Hohn, D. Veitch, K. Papagiannaki and C. Diot, 2004. Bridging router performance and queuing theory. Proceeding of the ACM SIGMETRICS/Performance, June 12-16, ACM, New York, USA., pp: 355-366. http://portal.acm.org/citation.cfm?id=1005686.1005728.
2. Imad Antonios and Lester Lipsky 2003. A performance model of user delay in on/off heavy-tailed traffic. The Proceedings of the 2nd International Symposium on Networt Computing and Applications, Apri. 16-18, IEEE Xplore, San Diego, CA., pp: 367-373. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1201177
3. Bradly, R. Smith and J.J. Garcia-Luna-Aceves, 1996. Securing the border gateway routing protocol. Proceedings of Global Internet'96, Nov. 1996, London, UK.., pp: 81-85. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.32.4651.
4. Jeff Doyle and Jennifer Carroll, 2005. CCIE Professional Development Routing TCP/IP. 2nd Edn., Published by Cisco Press, pp: 936. ISBN: 1587052024.

5. Scott Ballew, M. 1997. Managing IP Networks with Cisco Routers. 1st Edn., O'Reilly Media, Inc., Lawrence, MA, United States, pp: 334. ISBN: 1565923200.
6. Bob, A., J.J. G.L. Aceves and J. Boyle, 1994. EIGRP-a fast routing protocol based on distance vectors. Proceeding of Networld/Interop, May 1994, Las Vegas, NV, USA. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.24.645.
7. Houlden, N. V. Grout, J. McGinn and J. Davies, 2006. Extended end-to-end cost metrics for improved dynamic route calculation. Proceedings of the 6th International Network Conference INC2006, University of Plymouth UK., pp: 89-96. http://www.glyndwr.ac.uk/groutv/Papers/P1.pdf.
8. Ivan Pepelnjak, 2000. EIGRP Network Design Solutions. 1st Edn., Published by Cisco Press, US., pp: 366. ISBN-10: 1578701651.
9. Chandramouli, R. T. Grance, R. Kuhn and S. Landau, 2006. Toward secure routing infrastructures. Proceedings of the IEEE Security and Privacy, IEEE Computer Society, pp: 1540-7993.
10. Kwok Fung, T. 2004. Network Security Technologies. 2nd Edn., Auerbach Publications CRC Press, FL., pp: 273. ISBN: 0849330270.
11. Merike Kaeo, 2003. Designing Network Security. 2nd Edn., Cisco Publications Press, pp: 768. ISBN: 1587051176.
12. Rivest, R. 1992. The MD5 Message-Digest Algorithm. http://portal.acm.org/citation.cfm?id=RFC1321.
13. Al-Saud, A.K. H.M.Tahir, A. Elzoghabi and M. Saleh, 2008. Performance evaluation of secured versus non-secured eigrp routing protocol. Proceeding of SAM, July 14-17, Las Vegas, NV., http://www.linkedin.com/pub/6/632/27.
14. Huang, D. A. Sinha and D. Medhi, 2003. A double authentication scheme to detect impersonation attack in link state routing protocols. The Proceedings of IEEE International Conference on Communications (ICC), May 11-15, Anchorage, Alaska, pp: 1723-1727. DOI: 10.1109/ICC.2003.1203895.
15. Deepakumara, J. H.M. Heys and R. Venkatesan. 2001. FPGA implementation of MD5 hash algorithm. The Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering CCECE, May 13-16, Toronto, Ontario, Canada, pp: 919-924. DOI: 10.1109/CCECE.2001.933564 .
16. F. Baker and R. Atkinson, 1997. RIP-2: MD5 Authentication. http://portal.acm.org/citation.cfm?id=RFC2082.
17. F. Baker and R. Atkinson, October 1994. OSPF MD5 Authentication. http://tools.ietf.org/html/draft-ietf-ospf-md5-01.