A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2, and OSPF

Khalid Abu Al-Saud[1, 2], Hatim Tahir[2], Moutaz Saleh[1], and Mohammed Saleh[1]
[1]Department of Computer Science and Engineering College of Engineering, Qatar University, Qatar
[2]Department of Computer Science, Faculty of Information Technology, Malaysia

Abstract: *Routing is the process of forwarding data across an inter-network from a designated source to a final destination. Along the way from source to destination, at least one intermediate node is considered. Due to the major role that routing protocols play in computer network infrastructures, special cares have been given to routing protocols with built-in security constraints. In this paper, we conduct performance evaluation comparisons on message digest 5 authenticated routing traffic with respect to EIGRP, RIPv2 and OSPF protocols. A network model of four Cisco routers has been employed with an ON/OFF traffic model used to describe text files transmissions over the network. Eventually, analysis tool has been developed and used to measure the average delay time and average jitter. The collected results show that the average delay time and jitter in the secured message digest 5 case can become significantly larger when compared to the non-secured case even in steady state conditions. Among all, the secured OSPF protocol shows the highest performance even when the system is extremely overloaded.*

Keywords: *Performance, MD5, EIGRP, RIPv2, and OSPF.*

Received November 3, 2008; accepted February 25, 2009

1. Introduction

As our economy and massive infrastructure increasingly rely on the Internet, routing protocols become of critical importance. Routing protocols, however, are difficult to efficiently secure; since an attacker may attempt to inject forged routing messages into the system or may modify legitimate routing messages sent by other sources. Routing protocols are, thus, subject to threats and attacks that can harm individual users or the network operations as a whole. For instance, an attacker may attack messages that carry control information in a routing protocol to break a routers' neighbouring relationship. This type of attack can impact the network routing behaviour in the affected routers and likely the surrounding neighbourhood as well. Attackers can also send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn could degrade the functionality of the router [11, 14, 17].

In addition, with almost free flow of information and the high availability of most resources, owners and managers of enterprise networks have to understand all the possible threats to their networks. These threats take many forms, but all result in loss of privacy to a certain degree and possibly malicious destruction of information or resources that can lead to large monetary losses. A threat is then defined as a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [10, 21].

Consequently, routing security has received varying levels of attention over the past several years [2, 5, 19], and has recently begun to attract more attention specifically around the public network. Due to its dynamically changing topology, open environment and lack of centralized security infrastructure, a routing protocol is extremely vulnerable to malicious node presence and to certain types of attacks that can occur. Thus, the ongoing work on requirements for the next generation routing system and future work on the actual mechanisms for it will require well documented routing security requirements.

In this paper, we will conduct performance evaluation study on Message Digest (MD5) authenticated routing traffic with respect to EIGRP, RIPv2 and OSPF protocols. A network model of four Cisco routers will be employed with an ON/OFF traffic model used to describe text files transmissions over the network. To collect the performance measures of interest, analysis tool will also be developed and used to measure the average delay time, average jitter and average throughput.

The remainder of the paper is organized as follows. Section 2 shows the previous research work on routing authentication. The adopted authentication technique, namely the MD5, used to secure EIGRP, RIPv2 and

OSPF routing protocols will be explained in section 3. Section 4 presents the physical network model proposed for this work and outlines its setup and configurations. The system model and traffic model are also illustrated here, before the collected results are strictly discussed. Lastly, section 5 summarizes this research work.

2. Related Work

The current state of the ability in protecting the routing infrastructures relies on so-called best practices, which include various simplistic techniques such as passwords, TCP, authentication, route filters, and private addressing to ease the most basic vulnerabilities and threats [14, 21]. Authentication occurs when two neighbouring routers exchange routing information and ensures that the receiving router incorporates into its tables only the route information that the trusted sending neighbour really intends to send. It prevents a genuine router from accepting and then using unauthorized, malicious, or corrupted routing updates that may compromise the security or availability of the network. Such a compromise would lead to rerouting of traffic, or a denial of service.

For routing protocols to prevent such attacks, we must ensure that routers form peering or neighbouring relationships with trusted peers. One way to do this is by authenticating routing protocol messages. The EIGRP, RIPv2, and OSPF protocols support MD5 authentication, which uses a secret key combined with the data being protected to compute a hash. When the protocols send messages, the computed hash is transmitted with the data. The receiver uses the matching key to validate the message hash.

In a system as large as today's Internet, faults and attacks are inevitable. Given that all Internet based communications rely on a dependable packet delivery service, it is critically important to make network routing protocols highly secured [4]. Consequently, the past decade witnessed a number of research works on this area. For instance, [1] analyzed the security of the Border Gateway Protocol (BGP) routing protocol, and identify a number of vulnerabilities in its design and the corresponding threats. The authors presented a set of proposed modifications to the protocol which minimize or eliminate the most significant threats. Also, [3] described how to achieve hop integrity in networks that support Internet Protocol (IP). The authors adopted two famous protocols used in IP networks, namely RIP and OSPF to illustrate how hop integrity can secure the communications between adjacent routers.

Traditional routing protocol designs have focused solely on the functionality of the protocols and simplicity assumes that all routing update messages received by a router carry valid information. However, operational experience suggests that hardware faults and operator miss-configurations can all lead to invalid routing protocol messages. Thus, the authors in [5] developed a simple and effective approach to detect invalid routing messages in RIP routing protocol. Their design emphasizes effectiveness, simplicity, low overhead, backward compatibility with the standard RIP protocol, and supports for incremental deployment.

Furthermore, in [20] a survey made on the research efforts over the years aimed at enhancing the dependability of the routing infrastructure. To provide a comprehensive overview of these various efforts, the research work introduced a threat model based on known threats, then sketched out a defense framework. The analysis shows that although individual defense mechanisms may effectively guard against specific faults, no single fence can counter all faults. Also, the analysis shows that in order to provide secured neighbourhood communication then plaintext passwords and keyed MD5 authentication are needed. Plaintext passwords are vulnerable to eavesdropping, while keyed MD5 authentication can effectively protect neighbourhood protocol exchanges.

In the area of distance vector routing protocols, the research work in [4] proved that such existing protocols are insecure due to the lack of strong authentication and authorization mechanisms and the difficulty, if not impossibility, of validating routing messages which are aggregated results of other routers. Consequently, the authors introduced a secure routing protocol, namely secured-RIP, based on a distance vector approach. In secured-RIP, a router confirms the consistency of an advertised route with those nodes that have propagated that route. The threat analysis and simulation results showed that in secured-RIP, a well-behaved node can uncover inconsistent routing information in a network with many misbehaving nodes assuming no two of them are in collusions, with relatively low extra routing overhead.

3. MD5 Routing 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 MD5, route filters, and private addressing [16]. Authentication occurs when any router ensures that only routing updates received from a trusted neighbour 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 [18].

The well known MD5 algorithm [12] 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 Figure 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.

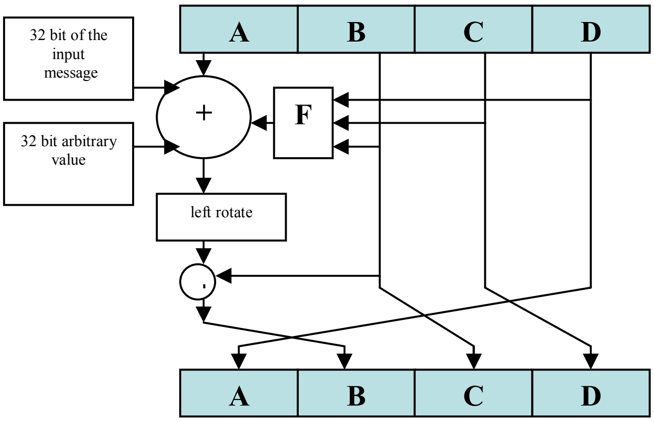


Figure 1. MD5 Algorithm; F is a nonlinear function of (B, C, and D).

Most routing protocols incorporate MD5 neighbor authentication to protect the integrity of the routing domain. Authentication occurs when two neighboring routers exchange routing information and ensures that the receiving router incorporates into its tables only the route information that the trusted sending neighbor really intends to send. This prevents a legitimate router from accepting and then using unauthorized, malicious, or corrupted routing messages that may compromise the security or availability of the network. Such a compromise would lead to rerouting of traffic, a denial of service, or just giving access to certain packets of data to an unauthorized person.

In MD5 authentication, the participating routers must share an authentication key. This key must be manually preconfigured on each router. In particular, EIGRP, RIPv2 and OSPF routing protocols are supported with 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.

For EIGRP, multiple keys which are grouped into one keychain 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. EIGRP MD5 authentication ensures that routers accept EIGRP packets only from trusted sources. After the MD5 authentication is configured on an interface, every EIGRP packet sent by a router over that interface is signed with an MD5 fingerprint. Now, every EIGRP packet received over an interface with MD5 authentication configured is checked to verify that the MD5 fingerprint in the packet matches the expected value, making it impossible for the intruder to insert un-trusted routers in the network or send false packets to the routers.

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. The RIPv2 authentication key is selected by the sender based on the outgoing interface. Each key has a lifetime associated with it, and no key is ever used outside its lifetime. Table 1 depicts the steps to be carried out at the sending router to generate an authenticated RIP message, while Table 2 depicts the steps to be carried out at the destination router to retrieve the MD5 digest.

Table 1. Generating an authenticated RIP message.

Step 1	The Authentication Offset, Key Identifier, and Authentication size fields are appropriately filled.
Step 2	The 16-byte keyed MD5 RIPv2 authentication key is appended to the data.
Step 3	The trailing Pad and Length fields are added and the digest calculated using the MD5 algorithm.
Step 4	The 16 byte digest is written over the RIPv2 authentication key.

Table 2. Retrieving MD5 digest.

Step 1	The digest is kept in memory.
Step 2	The appropriate algorithm and key are determined from the Key Identifier.
Step 3	The RIPv2 16 byte authentication key is written into the appropriate number of bytes starting at the indicated offset.
Step 4	Appropriate padding is added, and then a new digest is calculated using MD5 algorithm.

All OSPF protocol exchanges are authenticated. The OSPF packet header includes an Authentication Type field and 64 bits of data to be used by the appropriate authentication scheme. Each OSPF 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 [9, 8]. The OSPF checksum is computed over the whole OSPF packet, excluding the 8-byte Authentication field. The Authentication Type field, which is configurable on a router per-interface basis, identifies the authentication algorithm [7]. Figure 2 illustrates the sequence of events involved in MD5 authentication at the sending router.

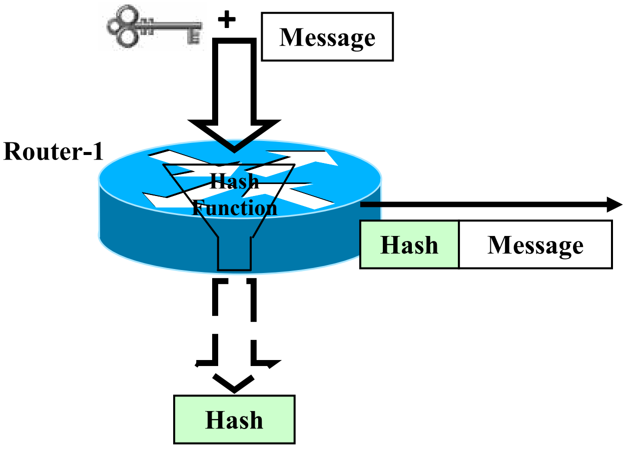


Figure 2. MD5 Neighbour authentication at the sending router.

The MD5 algorithm takes the preconfigured shared secret key and the traffic data, message, as inputs and returns a message digest or hash that is appended to the message and sent through the appropriate interface [6]. The destination router takes the routing information, along with its preconfigured shared secret, and uses this as input to the MD5 algorithm to produce a message digest. If this new digest matches the one that was received, the neighbour is authenticated and the routing information is incorporated into the router's routing information. Figure 3 illustrates the sequence of events for routing protocol authentication at the destination router.

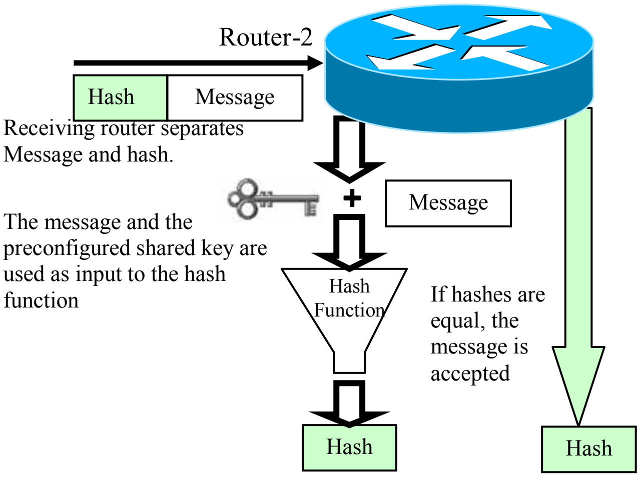

Router-2
Hash
Message
Receiving router separates Message and hash.
+
Message
The message and the preconfigured shared key are used as input to the hash function
Hash Function
If hashes are equal, the message is accepted
Hash
Hash

Figure 3. The sequence of events at the destination router.

Following next, we present in details the real experiment network model we adopt for evaluating the performance of the selected routing protocols in the context of secured MD5 authentication versus non-secured situations before we strictly discuss the collected experimental results.

4. The Study

The main objective of our work is to study the performance of selected commonly-used protocols, namely: EIGRP, RIPv2 and OSPF, with/without MD5 authenticated network traffic on various scales of network models and with various traffic patterns. Our initial idea was to monitor and capture a plugged traffic in a simulated network model. Unfortunately, none of the available simulators support required authentication commands that are essential to this study. Therefore, we decided to conduct out study experimentally under constrains of scalability, and resources availability in our research lab. Our first step is to construct a network model consisting of physical Cisco 1721 routers and attached terminals. Next, we plug traffic into the network model and study the performance measures of interest by capturing necessary data. The subsequent sections describe in details the system including: physical network model, system model and used traffic pattern.

4.1. The Physical Network Model

Our network model consists of four Cisco 1721 modular access routers with attached terminals. A terminal connected to ROUTER3 will be used to plug directed traffic into the network; this terminal will be called the Client. While, the terminal connected to ROUTER2 is the targeted recipient of the traffic plugged by the Client, this terminal will be called the Server. Both the Client and the Server are connected to their associated routers 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 800,000Hz. Figure 4 shows the detailed configurations of the network model.

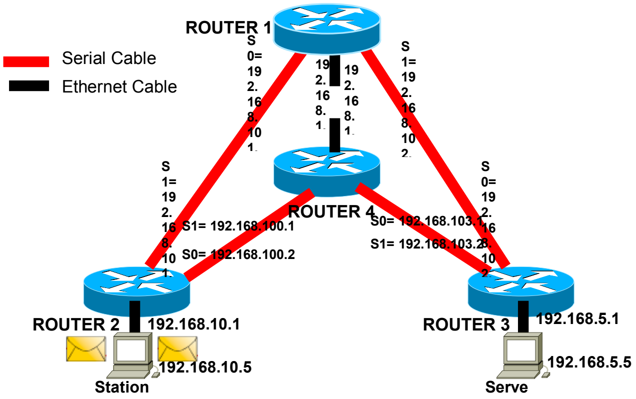


Figure 4. The proposed test-bed network model of Cisco routers.

The configuration instructions of the routing protocols on the routers can be found in [13]. It worth saying that a keychain and at least one key must be created in order to enable authentication to provide secured routing updates.

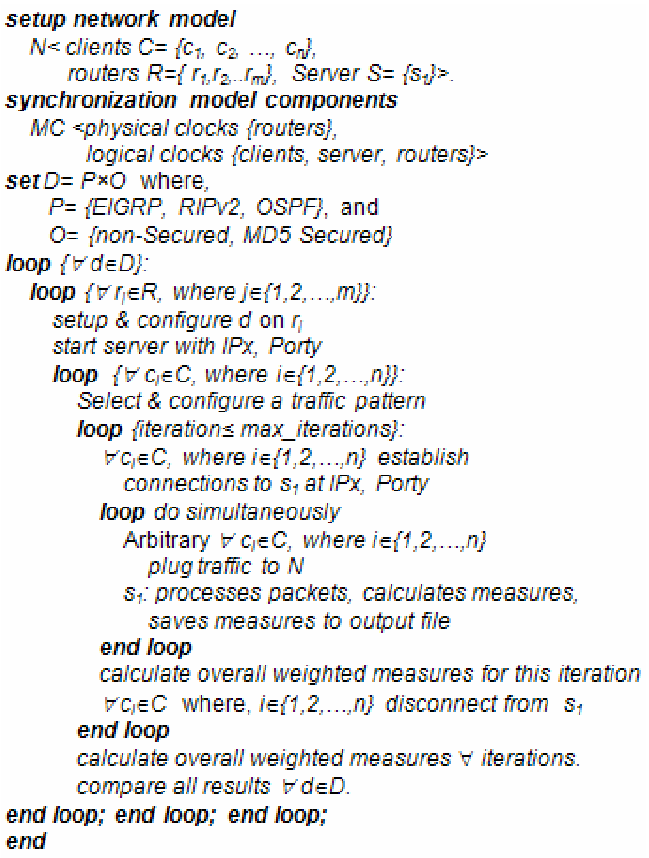
The hardware clock of individual routers initially was not synchronized. To overcome this problem, we configured ROUTER1 to host Server Network Time

Protocol (SNTP).The remaining routers are configured to adjust their times based on the SNTP on ROUTER1. Another synchronization problem between the end-to-end nodes needed to be solved. We used ClockSynch tool from PMSystem [22] at the end nodes to synchronize their clocks with the rest of the network model components.

4.2. The System Model

The generic system model is concerned with integrating, configuring and executing the software components on the hardware components of the network model *N< clients C= {c1, c2, …, cn}, routers R={ r1,r2,..rm}, Server S= {s1}>.*

The generic system model is shown in Figure 5. Having a network model of synchronized physical and logical clocks of all attached hardware components, the system performs repeated executions of simultaneous tasks for each configuration combination in P×O where, P= {EIGRP, RIPv2, OSPF}, and O= {non-Secured, MD5 Secured}.



```
setup network model
  N< clients C= {$c_1$, $c_2$, …, $c_n$},
     routers R={ $r_1$,$r_2$,..$r_m$}, Server S= {$s_1$}>.
synchronization model components
  MC <physical clocks {routers},
       logical clocks {clients, server, routers}>
set D= P×O where,
    P= {EIGRP, RIPv2, OSPF}, and
    O= {non-Secured, MD5 Secured}
loop {$\forall$ d$\in$D}:
  loop {$\forall$ $r_j$$\in$R, where j$\in${1,2,…,m}}:
    setup & configure d on $r_j$
    start server with IPx, Porty
    loop {$\forall$ $c_i$$\in$C, where i$\in${1,2,…,n}}:
      Select & configure a traffic pattern
      loop {iteration$\leq$ max_iterations}:
        $\forall$$c_i$$\in$C, where i$\in${1,2,…,n} establish
          connections to $s_1$ at IPx, Porty
        loop do simultaneously
          Arbitrary $\forall$ $c_i$$\in$C, where i$\in${1,2,…,n}
            plug traffic to N
          $s_1$: processes packets, calculates measures,
            saves measures to output file
        end loop
        calculate overall weighted measures for this iteration
        $\forall$$c_i$$\in$C where, i$\in${1,2,…,n} disconnect from $s_1$
      end loop
      calculate overall weighted measures $\forall$ iterations.
      compare all results $\forall$d$\in$D.
end loop; end loop; end loop;
end
```

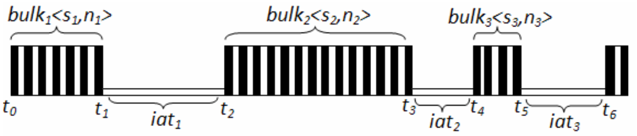
Figure 5. A general system model.

For each execution, an arbitrary number of clients plug their traffic into the network via the attached link with their designated routers targeting an attached terminal known as the server. The traffic is generated following java pre-implemented traffic models running on the attached clients. On the other end, the server computes the delay, jitter, and throughput then averages these values at the end of each execution and reports it in a file. Each scenario of the executions is repeatedly iterated to obtain the significant overall averages for the collected performance measurements of interest.

Finally, collected results for all combinations in *P×O* are tabulated and plotted for comparison study. In the next section, a traffic pattern best describing transmissions of files of various sizes is presented.

4.3. The Traffic Model

The traffic model used for this study best describes text traffic of files transmissions over the network. Periodically, files are transmitted over the network knowing that the times at which these transmissions are instantiated mark times for the establishments of bulks of packets sessions. The time periods of these bulks depend on the sizes of the files to be transmitted at each point of time, the capacity of the associated links, associated transmission delays and error rates. The sizes of the files are exponentially distributed with a mean of a number of bytes. A bulk session is described by distributing the bytes of the file to be transmitted in packets of a specific type of a specific payload which is highly reflected on the number of packet to be transmitted for that bulk session. Having a dynamic model, the transmission rate is variable represented by two types of periods namely ON and OFF periods. The lengths of the ON periods is controlled by the time needed to transmit the file corresponds to that period, while the lengths of the OFF periods is exponentially distributed. In other words, times of active session are apart exponentially, i.e., active sessions are Poisson with an activation rate or files arrival rate. Finally, the continuity of the traffic being alive is timely controlled. Figure 6 below summarizes our discussion on this traffic pattern.



iat_1, iat_2, iat_3, … are exponentially distributed inter bulks times.
s_1, s_2, s_3, … are exponentially distributed file sizes of corresponding bulks.
n_1, n_2, n_3, … are number of packets in corresponding bulks.
t_1, t_2, t_3, … times at which sessions are activated/deactivated.

Figure 6. The traffic model.

The traffic pattern is instantiated with Poisson arrivals of four files per second, i.e., inter time of active transmissions of packets bulks is exponentially distributed with mean equals to 250 milliseconds. The experiment is repeated for various exponentially distributed files sizes with means equal to 15, 30, 45… 100 Kbytes. The number of packets for each bulk is determined by distributing the data of the files on packets of payload equals to 1478 bytes. The traffic pattern is executed for 300 seconds for each experiment.

4.4. Experimental Results

In this research, four graphs were plotted to evaluate the average delay time and average jitter in *ms* with respect to the transmitted mean file size in *KB* for the three routing protocols. Various text traffic file, sent during the sessions of the ON periods, have been plugged into the simulation model. Initially, 15KB mean file size is loaded into the system and dramatically incremented with 15KB towards 100KB each iteration. Figure 7 shows the average delay time with mean file size in the non-secured case of EIGRP, RIPv2, and OSPF routing protocols.

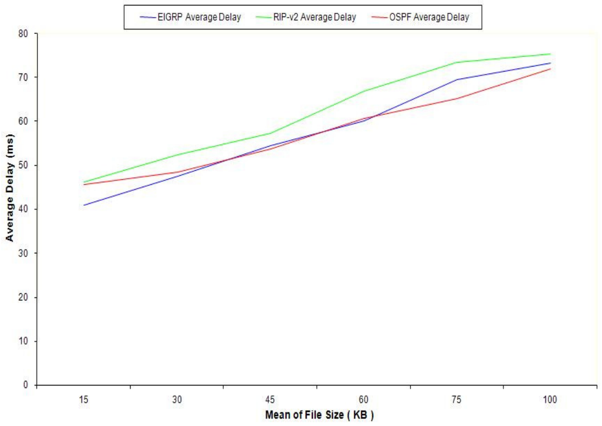


Figure 7. Average delay time in non-secured case.

The results show the average delay time of RIPv2 is obviously 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 above 60KB file size transmission.

Figure 8 shows the average delay time with mean file size in the secured MD5 case of EIGRP, RIPv2, and OSPF routing protocols. The results show that when the system is lightly loaded, all routing protocols give almost the same average delay values. Particularly, the OSPF protocol keeps the minimum values throughout the simulation benefiting from its link state routing properties in reducing packet processing time.

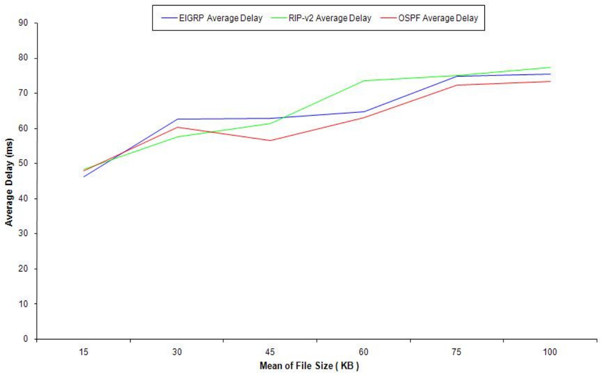


Figure 8. Average delay time in MD5 secured case.

Figure 9 shows the average jitter with mean file size in the non-secured case of EIGRP, RIPv2, and OSPF routing protocols. The results show that in the case of lightly loaded conditions, the OSPF routing protocol records a remarkable minimum average delay when compared with both RIPv2 and EIGRP due to its link state properties. However, starting the moderately loaded conditions and onwards the three routing protocols preserve the same jitter values in inversely proportional fashion with respect to the mean file size.

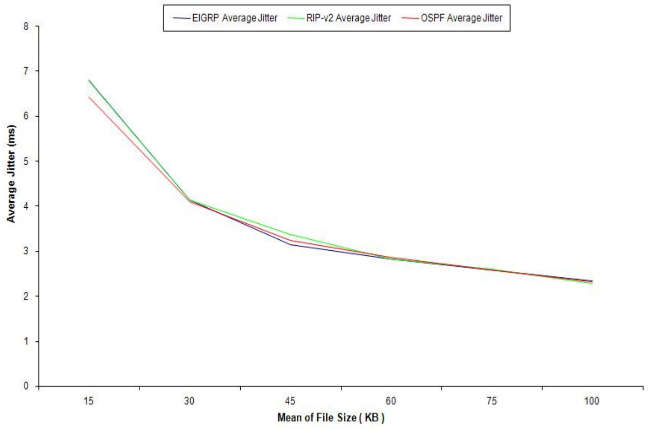


Figure 9. Average jitter time in non-secured case.

Figure 10 shows the average jitter with mean file size in the secured MD5 case of EIGRP, RIPv2, and OSPF routing protocols. The results show that throughout the whole experiment, the three routing protocols almost show the same results with very small variation. In general, OSPF and EIGRP protocols lead to higher performance in both secured and non-secured cases when compared to the RIPv2 protocol.

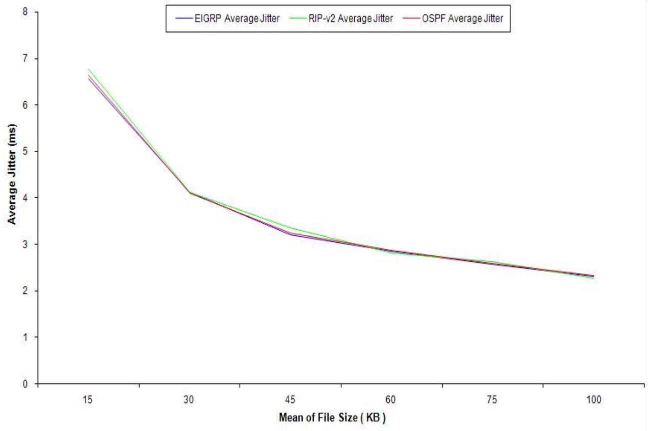


Figure 10. Average jitter time in MD5 secured case.

We can also conclude that link state routing protocols, represented by OSPF, are always better performed than distance vector routing protocols mainly represented by RIPv2. 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. Conclusions

Most routing protocols incorporate MD5 neighbor authentication to protect the integrity of the routing domain. This prevents a legitimate router from accepting and then using unauthorized, malicious, or corrupted routing messages that may compromise the security or availability of the network. In this paper, we conducted a comparison study on selected commonly-used protocols, namely: EIGRP, RIPv2 and OSPF, with/without MD5 authenticated network traffic on various network models scales and with various traffic patterns. Initially, we constructed a network model consisting of physical Cisco 1721 routers and attached terminals. Next, we plugged traffic into the network model and studied the performance measures of interest by capturing necessary data. The obtained experimental results showed that the average delay time and average jitter in the secured case can become significantly larger when compared to the non-secured case even in steady state conditions. However, the OSPF protocol shows the better performance by achieving the minimum average delay and average jitter even when the system is extremely overloaded.

Acknowledgements

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

References

[1] Bradly R., Smith J., and Garcia L., "Securing the Border Gateway Routing Protocol," *in Proceedings of the ISOC Symposium on Network and Distributed System Security*, UK, pp. 57-73, 1997.

[2] Bradly R. and Garcia A., "Securing the Border Gateway Routing Protocol," *in Proceedings of Global Internet'96*, UK, pp. 81-85, 1996.

[3] Dan P., Huang N., and Elnozahy G., "Hop Integrity and the Security of Routing Protocols," *in Proceedings of the 13th Annual Computer Security*, USA, pp. 308-319, 2002.

[4] Dan P., Lixia Z., and Dan M., "A Framework for Resilient Internet Routing Protocols," *Computer Journal of IEEE Network*, vol. 4, no. 1, pp. 1-36, 2004.

[5] Dan P., Dan M., and Lixia Z., "Detection of Invalid Routing Announcements in RIP Protocol," *in Proceeding in GLOBECOM IEEE*, UK, pp. 1237-1240, 2003.

[6] Deepakumara M. and Venkatesan R., "FPGA Implementation of MD5 Hash Algorithm," *in Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering*, Canada, pp. 919-924, 2001.

[7] Dijiang H., Amit S., and Deep M., "A Double Authentication Scheme to Detect Impersonation Attack in Link State Routing Protocols," *in Proceedings of IEEE International Conference on Communications*, Alaska, pp. 1723-1727, 2003.

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

[9] Feldmeier B. and Atkinson R., "RIP-2: MD5 Authentication IETF RFC2082," *Cisco Systems*, United States, pp. 12, 1997.

[10] Gert De L. and Gert S., *Network Security Fundamentals*, Publisher Cisco Press, 2004.

[11] Imad A. and Lester L., "A Performance Model of User Delay in On/Off Heavy-Tailed Traffic," *in Proceedings of The International Symposium on Performance Evaluation of Computer and Telecommunication Systems*, San Diego, pp. 11-12, 2002.

[12] Khalid S., Hatim T., Elzoghabi A., and Mohammad S., "Performance Evaluation of Secured Versus Non-Secured EIGRP Routing Protocol," *in Proceedings of SAM*, USA, pp. 174-178, 2008.

[13] Khalid S., Hatim T., Moutaz S., and Mohammed S., "Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 and OSPF," *Computer Journal of Computer Science*, vol. 4, no. 9, pp. 721-728, 2008.

[14] Merike K., *Designing Network Security,* Cisco Press, 2003.

[15] Papagiannaki K., Honn N., Hohn N., Veitch D., and Diot C., "Bridging Router Performance and Queuing Theory," *in Proceedings of ACM SIGMETRICS/Performance*, USA, pp. 355-366, 2004.

[16] Ramaswamy C., Tim G., Rick K., and Susan L., "Toward Secure Routing Infrastructures," *in Proceedings IEEE Security and Privacy*, *IEEE Computer Society*, Kwok Fung, pp. 1540-7993, 2006.

[17] Ravi M., *IP Routing: O'Reilly Online Catalog*, O'Reilly & Associates, 2002.

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

[19] Scott M., *Managing IP Networks with Cisco Routers, O'Reilly Online Catalog,* O'Reilly & Associates, 1997.

[20] Tao K. and Van O., "S-RIP: A Secure Distance Vector Routing Protocol," *in Proceedings of Applied Cryptography and Network Security,* China, pp. 8-11, 2004.

[21] Vnand A. and Chakrabarty K., *Cisco IP Routing Protocols: Troubleshooting Techniques*, Charles River Media, 2004.

[22] www. karjasoft. com /files/ clocksync1.0. 0exe, Last Visited 2008.

Khalid Abu Al-Saud received his BSc in computer systems engineering in 1988 from Al-Azhar University, Egypt. Currently, he is doing Master study at UUM, Malaysia. He holds the CCNA, MCSE, ICDL, and CTP international industry certificates. His main research interests include network security and routing protocols.

Hatim Tahir is an associate professor in the Department of Computer Science at University Utara Malaysia. He has more than 20 years of teaching experience and research works in various academic institutions. He published books on data communication and communication technology. He was formerly an expert member for Malaysian CyberSecurity panel. His research interest focuses on network security and intrusion detection systems.

Moutaz Saleh is a lecturer in the Department of Computer Science and Engineering at Qatar University. He earned his PhD in computer networking in 2008 from UKM, Malaysia. He is a Cisco certified internetwork expert who served various networking positions and published many research papers in reputable international journals and conferences. His main research interests include network scheduling and routing, real-time systems, and distributed systems.

Mohammad Saleh is an associate professor in the Department of Computer Science and Engineering at Qatar University. He was earned his PhD in computer networking in 2001 from UPM, Malaysia. He served the education field since the year of 1995 in various scholarly institutions. His research interest includes but not limited toperformance evaluation of computer networks of various scales and specialities, distributed systems, real-time systems, and modelling & simulations.