Performance Evaluation of Secured versus Non-Secured EIGRP Routing Protocol

Khalid Abu Al-Saud[1, 2], Hatim Mohd Tahir[2], Adel A. El-Zoghabi[1], and Mohammad Saleh[1]
[1]Dept. of CS & Engineering, College of Engineering, Qatar University, P.O. Box 2713 Doha, QATAR
[2]Dept. of Computer Science, Faculty of Information Tech., Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, 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 evaluate the performance of EIGRP routing protocol in the case of secured and non-secured routing traffic. This is done through studying and analyzing EIGRP routing traffic with and without security rules. A network model of four Cisco routers, from both software and hardware perspectives, has been employed and a traffic generation and analysis tools have been developed and used to generate traffic data and to measure the delay for performance evaluation. The results show that the average delay in the secured case can become significantly larger than the unsecured case even in steady state conditions. The differences between the delays are exponential and reach a steady state towards the end of the experiment.*

Keywords: EIGRP, Routing Updates, Performance Evaluation, and Secured Routing Updates.

1 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.

Over the past few years, a number of research works have been done in routing [1], [2], and [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 work 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 paper, we will evaluate the performance of EIGRP 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 for performance evaluation.

The remainder of the paper is organized as follows. Section 2 describes the EIGRP routing protocol. Section 3 presents the authentication technique used to secure the EIGRP, namely the MD5 authentication. Section 4 presents the real model of Cisco routers proposed in this work and outlines the operations and the interactions among the four routers. Section 5 is about the results of our experimental work and the performance evaluation. Finally, in Section 6 we summarize our current work, and lay down the milestones for the future work.

2 EIGRP routing protocol

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

$$C = \left(k_1 b + \frac{k_2 b}{256 - l} + k_3 d \right) \frac{k_3}{r - k_4}$$

where b is the minimum bandwidth measured in kilobits per second; l the load on the link expressed as a number from 0 to 255 (255 is 100 percent loading), d the total delay in unit of tens of milliseconds, and r the reliability along the length of the path 255 for 100 percent. $k1$, $k2$, $k3$, $k4$ and $k5$ are 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 $d = 256 d_0$, 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 $k1=1$, $k2=0$, $k3=1$, $k4=0$ & $k5=0$ 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.

3 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 [10].

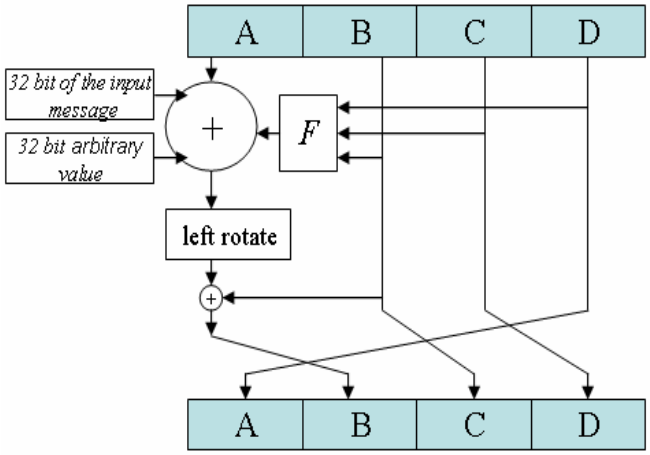

Figure 1: MD5 Algorithm; F: is a nonlinear function of (B, C, and D)

The well known MD5 algorithm [11] 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 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. Figure 2 illustrates the sequence of events involved in MD5 authentication for the sending router.

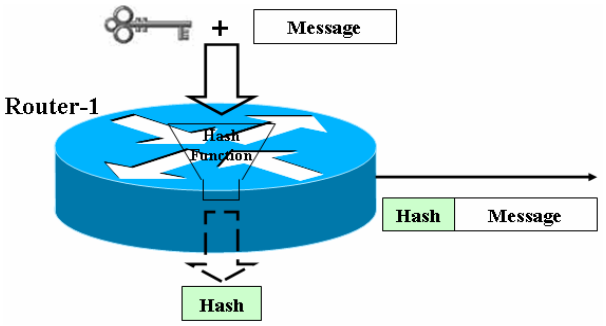

Figure 2: MD5 Neighbor Authentication at the Originating Router

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. Figure 3 illustrates the sequence of events for routing protocol authentication at the destination router.

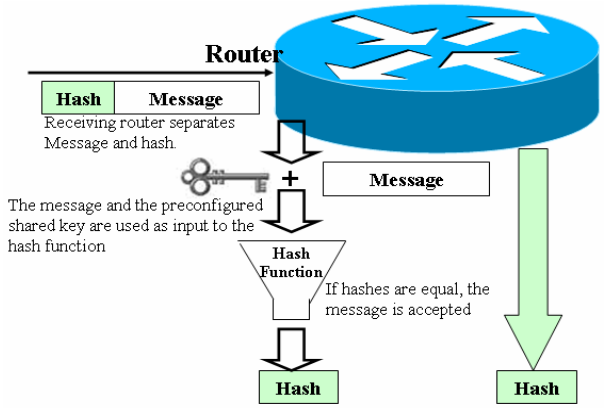

Figure 3: The Sequence of Events at the Destination Router

EIGRP supports only 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. 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 [12].

4 The test-bed network model

We intended to use available simulators to study the performance of EIGRP routing with and without security constraints. However, an intensive survey of the available simulators has revealed the fact that none of them supports authentication commands. Therefore, our network model has been experimentally implemented in our 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 are computed. This communication of traffic is implemented using a java client/server program running on terminals attached to the designated routers. In the next section, the experiment and simulation settings and configurations of the routers are explained in details.

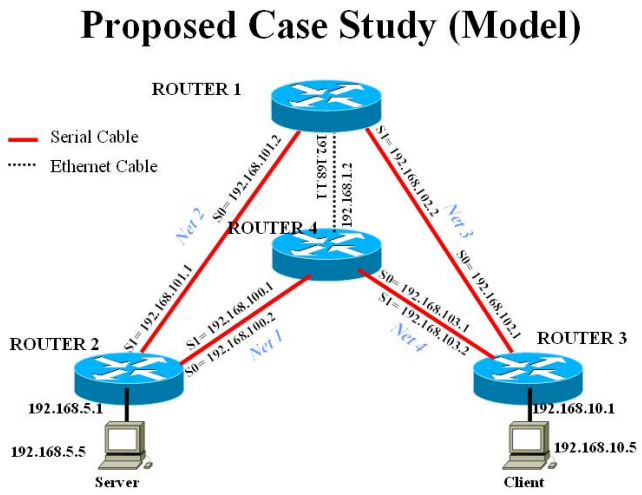

Figure 4: The Proposed Real Model of CISCO Routers

5 Experimental work and results

This section represents the actual experiment settings and routers configurations in both secured and unsecured modes. Simulation construction includes traffic patterns used, time synchronization among all routers, end client and server and other issues.

5.1 Setup and configuration of the routers

The test-bed network model is shown in Figure 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 Figure 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 following commands:

sntp server 192.168.102.2
sntp broadcast client

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 Figure 4.

Another major issue we faced the synchronization between the end-to-end nodes. For solving this problem, we used ClockSynch tool from PMSystem [13] at the end nodes to synchronize their clocks.

```
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 Serial1
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
```

Figure 5: ROUTER1 Configuration in the Unsecured Mode.

In the case where authentication is used, ROUTER1 configuration is shown in Figure 6. EIGRP routing authentication uses one secret key from the keychain as mentioned earlier. Before enabling authentication, a keychain and at least one key must be created. Creating a Keychain on ROUTER1 was done as follows:

On ROUTER1 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 this key as shown below:

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*

```
hostname ROUTER1
key chain khalidchain
 key 1
  key-string khalid-63
  accept-lifetime 00:00:00 Oct 31 2007 infinite
  send-lifetime 00:00:00 Oct 31 2007 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
interface Serial1
 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
```

Figure 6: ROUTER1 Configuration in the Secured Mode.

5.2 The experiment 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 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. 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.

5.3 Test-bed model results

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 50,000 packets.

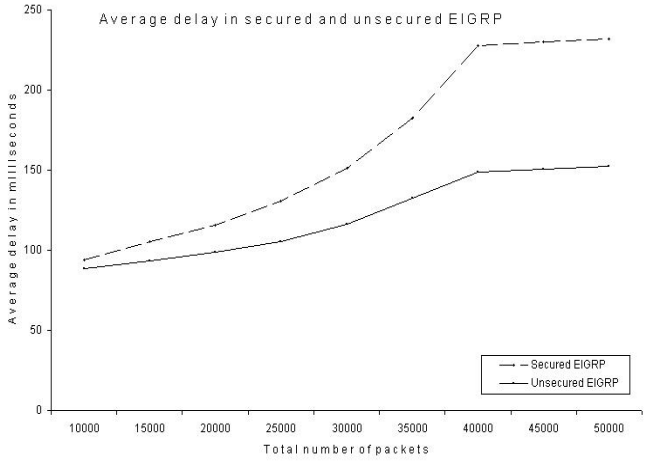

Figure 7: Average Delay in Secured MD5 Authentication and Unsecured EIGRP Routing Protocol

The results are shown in Figure 7, which indicates that the average delay in the secured case is continuously larger than it is in the unsecured case. The delay differences grow exponentially for the cases of 10,000 packets and up to 40,000 packets. At the point of 40,000 packets, the differences between the secured and unsecured cases tend to become almost constant indicating the steady-state of the system.

6 Conclusions and future work

In this paper, we studied the performance of secured versus non-secured EIGRP routing protocol. For secured routing protocol, we used MD5 authentication. We first described an actual model for carrying out the experiment. The lack of authentication support found in router simulators has forced us to use the real test-bed model. A Java client-server program for monitoring the traffic and reporting the delay time was presented as part of this work. The results obtained from the model and the program showed that the difference between the average delay in the secured case and the unsecured case has two phases: an exponential phase that ended at 40,000 packets, and a steady phase afterwards. During our investigation, we faced several problems, most notably the lack of simulators with built-in authentication commands and tools for synchronizing the client with the server.

As future extension of the work presented in this paper, we are planning to apply the same techniques to some other routing protocols and compare the performance, hopefully with some enhancements to the performance measuring simulation model.

Acknowledgement

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

7 References

[1] N Honn, D. et al. Bridging Router Performance and Queuing Theory. In proceeding of the International conference SIGMETRICS Performance '04, June 12-16 2004, New York.

[2] Imad Antonios. A Performance Model of User Delay in ON/OFF Heavy-Tailed Traffic, Proceedings in the 2002 International Symposium on Performance Evaluation of Computer and Telecommunication.

[3] Bradly R. Smith and J.J. Garcia-Luna. Securing the Border Gateway Routing Protocol, Proceedings of the ISOC Symposium on Network and Distributed System Security '97, February 11, 1997.

[4] Jeff Doyle, Jennifer Carroll, CCIE Professional Development Routing TCP/IP, Volume I, Second edition, Cisco Press, October 19, 2005.

[5] Scott M. Ballew. Managing IP Networks with Cisco Routers. 1st Edition October 1997.

[6] R. Albrightson and J.J. Garcia-Luna-Aceves and J. Boyle, EIGRP – A fast routing protocol based on distance-vectors, in: Proceeding of Networld/Interop ’94, Las Vegas, NV, May 1994.

[7] Nigel Houlden, Vic Grout, John McGinn and John Davies, Extended End-to-End Cost Metrics for Improved, Dynamic Route Calculation, Proceedings of the 6th International Network Conference (INC 2006), University of Plymouth, 11-14 July 2006, pp89-96.

[8] Ivan Pepelnjak, EIGRP network design solutions Handbook. Cisco Press 2000.

[9] Ramaswamy Chandramouli, Tim Grance, Rick Kuhn, Susan Landau, Toward Secure Routing Infrastructures, Proceedings of the IEEE SECURITY & PRIVACY 2006, pages 84-78

[10] Kwok T. Fung, Network Security Technologies, CRC Press, 2nd Edition, 2005.

[11] R. Rivest, "The MD5 Message-Digest Algorithm", IETF RFC 1321.

[12] Merike Kseo, Designing Network Security, second edition, Cisco Press, October 30, 2003.

[13] www.karjasoft.com/files/clocksync/ClockSync1.0.0.exe, last visit 06/02/2008.