

# Ciências Exatas e da Terra e a Dimensão Adquirida através da Evolução Tecnológica 3

Jorge González Aguilera  
Alan Mario Zuffo  
(Organizadores)



**Jorge González Aguilera**

**Alan Mario Zuffo**

(Organizadores)

# Ciências Exatas e da Terra e a Dimensão Adquirida através da Evolução Tecnológica 3

Atena Editora  
2019

2019 by Atena Editora  
Copyright © Atena Editora  
Copyright do Texto © 2019 Os Autores  
Copyright da Edição © 2019 Atena Editora  
Editora Executiva: Profª Drª Antonella Carvalho de Oliveira  
Diagramação: Karine de Lima  
Edição de Arte: Lorena Prestes  
Revisão: Os Autores

O conteúdo dos artigos e seus dados em sua forma, correção e confiabilidade são de responsabilidade exclusiva dos autores. Permitido o download da obra e o compartilhamento desde que sejam atribuídos créditos aos autores, mas sem a possibilidade de alterá-la de nenhuma forma ou utilizá-la para fins comerciais.

### **Conselho Editorial**

#### **Ciências Humanas e Sociais Aplicadas**

Prof. Dr. Álvaro Augusto de Borba Barreto – Universidade Federal de Pelotas  
Prof. Dr. Antonio Carlos Frasson – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Antonio Isidro-Filho – Universidade de Brasília  
Prof. Dr. Constantino Ribeiro de Oliveira Junior – Universidade Estadual de Ponta Grossa  
Profª Drª Cristina Gaio – Universidade de Lisboa  
Prof. Dr. Deyvison de Lima Oliveira – Universidade Federal de Rondônia  
Prof. Dr. Gilmei Fleck – Universidade Estadual do Oeste do Paraná  
Profª Drª Ivone Goulart Lopes – Istituto Internazionele delle Figlie de Maria Ausiliatrice  
Prof. Dr. Julio Candido de Meirelles Junior – Universidade Federal Fluminense  
Profª Drª Lina Maria Gonçalves – Universidade Federal do Tocantins  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Profª Drª Paola Andressa Scortegagna – Universidade Estadual de Ponta Grossa  
Prof. Dr. Urandi João Rodrigues Junior – Universidade Federal do Oeste do Pará  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande  
Prof. Dr. Willian Douglas Guilherme – Universidade Federal do Tocantins

#### **Ciências Agrárias e Multidisciplinar**

Prof. Dr. Alan Mario Zuffo – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Alexandre Igor Azevedo Pereira – Instituto Federal Goiano  
Profª Drª Daiane Garabeli Trojan – Universidade Norte do Paraná  
Prof. Dr. Darllan Collins da Cunha e Silva – Universidade Estadual Paulista  
Prof. Dr. Fábio Steiner – Universidade Estadual de Mato Grosso do Sul  
Profª Drª Girlene Santos de Souza – Universidade Federal do Recôncavo da Bahia  
Prof. Dr. Jorge González Aguilera – Universidade Federal de Mato Grosso do Sul  
Prof. Dr. Ronilson Freitas de Souza – Universidade do Estado do Pará  
Prof. Dr. Valdemar Antonio Paffaro Junior – Universidade Federal de Alfenas

#### **Ciências Biológicas e da Saúde**

Prof. Dr. Benedito Rodrigues da Silva Neto – Universidade Federal de Goiás  
Prof.ª Dr.ª Elane Schwinden Prudêncio – Universidade Federal de Santa Catarina  
Prof. Dr. Gianfábio Pimentel Franco – Universidade Federal de Santa Maria  
Prof. Dr. José Max Barbosa de Oliveira Junior – Universidade Federal do Oeste do Pará

Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Profª Drª Raissa Rachel Salustriano da Silva Matos – Universidade Federal do Maranhão  
Profª Drª Vanessa Lima Gonçalves – Universidade Estadual de Ponta Grossa  
Profª Drª Vanessa Bordin Viera – Universidade Federal de Campina Grande

### **Ciências Exatas e da Terra e Engenharias**

Prof. Dr. Adélio Alcino Sampaio Castro Machado – Universidade do Porto  
Prof. Dr. Eloi Rufato Junior – Universidade Tecnológica Federal do Paraná  
Prof. Dr. Fabrício Menezes Ramos – Instituto Federal do Pará  
Profª Drª Natiéli Piovesan – Instituto Federal do Rio Grande do Norte  
Prof. Dr. Takeshy Tachizawa – Faculdade de Campo Limpo Paulista

### **Conselho Técnico Científico**

Prof. Msc. Abrãao Carvalho Nogueira – Universidade Federal do Espírito Santo  
Prof. Dr. Adaylson Wagner Sousa de Vasconcelos – Ordem dos Advogados do Brasil/Seccional Paraíba  
Prof. Msc. André Flávio Gonçalves Silva – Universidade Federal do Maranhão  
Prof.ª Drª Andreza Lopes – Instituto de Pesquisa e Desenvolvimento Acadêmico  
Prof. Msc. Carlos Antônio dos Santos – Universidade Federal Rural do Rio de Janeiro  
Prof. Msc. Daniel da Silva Miranda – Universidade Federal do Pará  
Prof. Msc. Eliel Constantino da Silva – Universidade Estadual Paulista  
Prof.ª Msc. Jaqueline Oliveira Rezende – Universidade Federal de Uberlândia  
Prof. Msc. Leonardo Tullio – Universidade Estadual de Ponta Grossa  
Prof.ª Msc. Renata Luciane Polsaque Young Blood – UniSecal  
Prof. Dr. Welleson Feitosa Gazel – Universidade Paulista

<b>Dados Internacionais de Catalogação na Publicação (CIP) (eDOC BRASIL, Belo Horizonte/MG)</b>	
C569	Ciências exatas e da terra e a dimensão adquirida através da evolução tecnológica 3 [recurso eletrônico] / Organizadores Jorge González Aguilera, Alan Mario Zuffo. – Ponta Grossa, PR: Atena Editora, 2019. – (Ciências Exatas e da Terra e a Dimensão Adquirida Através da Evolução Tecnológica; v. 3)  Formato: PDF Requisitos de sistema: Adobe Acrobat Reader Modo de acesso: World Wide Web Inclui bibliografia ISBN 978-85-7247-474-0 DOI 10.22533/at.ed.740191107  1. Ciências exatas e da terra – Pesquisa – Brasil. 2. Tecnologia. I. Aguilera, Jorge González. II. Zuffo, Alan Mario  CDD 509.81
<b>Elaborado por Maurício Amormino Júnior – CRB6/2422</b>	

Atena Editora  
Ponta Grossa – Paraná - Brasil  
[www.atenaeditora.com.br](http://www.atenaeditora.com.br)  
contato@atenaeditora.com.br

## APRESENTAÇÃO

A obra “*Ciências Exatas e da Terra e a Dimensão Adquirida através da Evolução Tecnológica vol. 3*” aborda uma publicação da Atena Editora, apresenta, em seus 23 capítulos, conhecimentos tecnológicos e aplicados as Ciências Exatas e da Terra.

Este volume dedicado à Ciência Exatas e da Terra traz uma variedade de artigos que mostram a evolução tecnológica que vem acontecendo nestas duas ciências, e como isso tem impactado a vários setores produtivos e de pesquisas. São abordados temas relacionados com a produção de conhecimento na área da matemática, química do solo, computação, geoprocessamento de dados, biodigestores, educação ambiental, manejo da água, entre outros temas. Estas aplicações visam contribuir no aumento do conhecimento gerado por instituições públicas e privadas no país.

Aos autores dos diversos capítulos, pela dedicação e esforços sem limites, que viabilizaram esta obra que retrata os recentes avanços científicos e tecnológicos nas Ciências Exatas e da Terra, os agradecimentos dos Organizadores e da Atena Editora.

Por fim, esperamos que este livro possa colaborar e instigar mais estudantes e pesquisadores na constante busca de novas tecnologias para a área da Física, Matemática, e na Agronomia e, assim, contribuir na procura de novas pesquisas e tecnologias que possam solucionar os problemas que enfrentamos no dia a dia.

Jorge González Aguilera

Alan Mario Zuffo

## SUMÁRIO

<b>CAPÍTULO 1</b> .....	<b>1</b>
ACURÁCIA TEMÁTICA DE DADOS GEOESPACIAIS CONFORME A ET-CQDG	
Rodrigo Wanderley de Cerqueira Ana Cláudia Bezerra de Albuquerque Borborema de Andrade Alex de Lima Teodoro da Penha Fábio Dayan Soares de Melo	
<b>DOI 10.22533/at.ed.7401911071</b>	
<b>CAPÍTULO 2</b> .....	<b>13</b>
UM PANORAMA GERAL SOBRE A CALIBRAÇÃO DINÂMICA DE TRANSDUTORES DE PRESSÃO PIZOELETRICOS	
Flávio Roberto Faciolla Theodoro Maria Luisa Colucci da Costa Reis Carlos D'Andrade Souto	
<b>DOI 10.22533/at.ed.7401911072</b>	
<b>CAPÍTULO 3</b> .....	<b>20</b>
ANÁLISE DE INTEGRIDADE ESTRUTURAL ATRAVÉS DE SISTEMAS IMUNOLÓGICOS ARTIFICIAIS	
Rafaela Pereira Segantim Mara Lúcia Martins Lopes Fábio Roberto Chavarette	
<b>DOI 10.22533/at.ed.7401911073</b>	
<b>CAPÍTULO 4</b> .....	<b>30</b>
ANÁLISE DAS CARACTERÍSTICAS DO PROTOCOLO DE ROTEAMENTO RIP: UM ESTUDO DE CASO SOBRE O ASPECTO DE SEGURANÇA NO RIPV2	
Charles Hallan Fernandes dos Santos Lucivânia da Silva Souza Felipe Sampaio Dantas Silva	
<b>DOI 10.22533/at.ed.7401911074</b>	
<b>CAPÍTULO 5</b> .....	<b>40</b>
ANÁLISES DA RESISTÊNCIA À CORROSÃO E ESQUEMAS DE PINTURAS EM CHAPAS DE AÇO ASTM A242 E AÇO CARBONO SAE 1020	
Rafaela Vale Matos	
<b>DOI 10.22533/at.ed.7401911075</b>	
<b>CAPÍTULO 6</b> .....	<b>45</b>
APLICAÇÃO DE ESFERAS DE QUITOSANA E ESFERAS DE QUITOSANA MODIFICADA COM NANOPÁRTÍCULA MAGNÉTICA (MAGNETITA) EM ANÁLISE DE ADSORÇÃO PARA O ÍON METÁLICO CROMO (VI)	
Andréa Claudia Oliveira Silva Maria José de Oliveira Pessoa	
<b>DOI 10.22533/at.ed.7401911076</b>	

<b>CAPÍTULO 7</b> .....	<b>55</b>
AVALIAÇÃO METROLÓGICA DE ANALISADORES DE QUALIDADE DE ENERGIA	
Rodrigo Rodrigues Nascimento Zampilis	
Marcelo Britto Martins	
<b>DOI 10.22533/at.ed.7401911077</b>	
<b>CAPÍTULO 8</b> .....	<b>62</b>
AXIOMAS FUNDAMENTAIS EM SISTEMAS DE MONITORAMENTO: UMA ANÁLISE EXPERIMENTAL PARA O MÉTODO DA IMPEDÂNCIA ELETROMECAÂNICA	
Caio Henrique Rodrigues	
Guilherme Silva Bergamim	
<b>DOI 10.22533/at.ed.7401911078</b>	
<b>CAPÍTULO 9</b> .....	<b>75</b>
VISÃO CEGA	
Vitoria Camargo da Silva	
Erinaldo Sanches Nascimento	
Fabiana Calisto Trevisan	
José Roberto Parra	
<b>DOI 10.22533/at.ed.7401911079</b>	
<b>CAPÍTULO 10</b> .....	<b>86</b>
CÉU ACESSÍVEL: APLICATIVO NA PLATAFORMA ANDROID PARA O ENSINO DE ASTRONOMIA PARA PESSOAS COM DEFICIÊNCIA VISUAL	
Ana Carolina Sampaio Frizzera	
Danielli Veiga Carneiro Sondermann	
Athyla Caetano	
Giovana Dewes Munari	
Caroline Azevedo Rosa	
Péricles José Ferreira	
Ronaldo Leffler	
Gabriel Barcellos Kretli Lopes	
<b>DOI 10.22533/at.ed.74019110710</b>	
<b>CAPÍTULO 11</b> .....	<b>97</b>
DETERMINAÇÃO TEÓRICA DO TEMPO DE ACELERAÇÃO EM 30 METROS PARA UM VEÍCULO BAJA SAE A PARTIR DO PRINCÍPIO DO IMPULSO	
Daiane Sampaio Fernandes	
Mateus Coutinho de Moraes	
Miguel Ângelo Menezes	
<b>DOI 10.22533/at.ed.74019110711</b>	
<b>CAPÍTULO 12</b> .....	<b>105</b>
DILATAÇÃO DE VEÍCULOS TANQUE RODOVIÁRIO	
Luciano Bruno Faruolo	
Edisio Alves de Aguiar Junior	
<b>DOI 10.22533/at.ed.74019110712</b>	

<b>CAPÍTULO 13</b> .....	<b>110</b>
EFEITO DA VARIAÇÃO DO VALOR DA DENSIDADE LATERAL RELACIONADA À SEPARAÇÃO GEOIDE-QUASEGEOIDE NA REGIÃO DE PORTO ALEGRE RS – ESTUDO DE CASO	
Roosevelt De Lara Santos Jr.	
<b>DOI 10.22533/at.ed.74019110713</b>	
<b>CAPÍTULO 14</b> .....	<b>118</b>
ELECTROCHEMICAL SENSING OF OH RADICALS AND RADICAL SCAVENGERS BASED ON POLY(METHYLENE BLUE)-MODIFIED ELECTRODE	
Maurício Hilgemann	
Marcelo Barcellos da Rosa	
<b>DOI 10.22533/at.ed.74019110714</b>	
<b>CAPÍTULO 15</b> .....	<b>131</b>
ESTUDO DA VIABILIDADE ECONÔMICA DE MICRO GERAÇÃO RESIDENCIAL EM UM AMBIENTE MICRO REDE, CONSIDERANDO DIFERENTES CENÁRIOS	
Luiz Guilherme Piccioni de Almeida	
<b>DOI 10.22533/at.ed.74019110715</b>	
<b>CAPÍTULO 16</b> .....	<b>141</b>
EXPRESSÃO GRÁFICA E OFICINAS PEDAGÓGICAS: CONTRIBUIÇÕES PARA A APRENDIZAGEM DE MATEMÁTICA BÁSICA	
Alessandra Assad Angieski	
Heliza Colaço Góes	
Davi Paula da Silva	
<b>DOI 10.22533/at.ed.74019110716</b>	
<b>CAPÍTULO 17</b> .....	<b>155</b>
LOGÍSTICA DA DESTINAÇÃO FINAL DOS RESÍDUOS SÓLIDOS DE SAÚDE DOS PRINCIPAIS HOSPITAIS DE ARACAJU/SE	
Ana Lúcia Oliveira Filipin	
Cleverton dos Santos	
Izabel Cristina Gomes de Oliveira	
Ana Sophia Oliveira Filipin	
<b>DOI 10.22533/at.ed.74019110717</b>	
<b>CAPÍTULO 18</b> .....	<b>161</b>
LUNAPPTICO: SOFTWARE DE TECNOLOGIA ASSISTIVA UTILIZADO NA COMUNICAÇÃO DE CRIANÇAS AUTISTAS DO ESTADO DO RN	
Elizeu Sandro da Silva	
Alyson Ricardo De Araújo Barbosa.	
Joêmia Leilane Gomes de Medeiros	
Welliana Benevides Ramalho	
Andrezza Cristina da Silva Barros Souza	
<b>DOI 10.22533/at.ed.74019110718</b>	

<b>CAPÍTULO 19</b> .....	<b>180</b>
MODELAGEM DE UM SISTEMA DE INFORMAÇÃO GEOGRÁFICA MÓVEL COLABORATIVO PARA DEFICIENTES FÍSICOS Sivoney Pinto Dias Helder Guimarães Aragão <b>DOI 10.22533/at.ed.74019110719</b>	
<b>CAPÍTULO 20</b> .....	<b>194</b>
MODELAGEM E PROGRAMAÇÃO DE UMA PLATAFORMA DE STEWART Rodolfo Gabriel Pabst Roberto Simoni Maurício de Campos Porath Milton Evangelista de Oliveira Filho Antônio Otaviano Dourado <b>DOI 10.22533/at.ed.74019110720</b>	
<b>CAPÍTULO 21</b> .....	<b>207</b>
SISTEMA DE NOTIFICAÇÕES POR MENSAGENS DE CELULAR PARA MONITORAMENTO EM ATIVOS DE REDE César Eduardo Guarienti Igor Breno Estácio Dutra de Oliveira Thiago H. da C. Silva Raphael de Souza Rosa Gomes <b>DOI 10.22533/at.ed.74019110721</b>	
<b>CAPÍTULO 22</b> .....	<b>213</b>
MONTAGEM DE UM ARRANJO EXPERIMENTAL DIDÁTICO PARA O ESTUDO DA ESPECTROSCOPIA DE IMPEDÂNCIA ELETROQUÍMICA Ernando Silva Ferreira Ricardo Macedo Borges Boaventura Juan Alberto Leyva Cruz <b>DOI 10.22533/at.ed.74019110722</b>	
<b>CAPÍTULO 23</b> .....	<b>225</b>
O NOVO (E ATUAL) SI E O SEU IMPACTO NA METROLOGIA ELÉTRICA NO BRASIL Regis Pinheiro Landim Helió Ricardo Carvalho <b>DOI 10.22533/at.ed.74019110723</b>	
<b>SOBRE OS ORGANIZADORES</b> .....	<b>240</b>

## ANÁLISE DAS CARACTERÍSTICAS DO PROTOCOLO DE ROTEAMENTO RIP: UM ESTUDO DE CASO SOBRE O ASPECTO DE SEGURANÇA NO RIPv2

### **Charles Hallan Fernandes dos Santos**

Diretoria Acadêmica de Gestão e Tecnologia da Informação (DIATINF) Campus Natal-Central

### **Lucivânia da Silva Souza**

Diretoria Acadêmica de Gestão e Tecnologia da Informação (DIATINF) Campus Natal-Central

### **Felipe Sampaio Dantas Silva**

Diretoria Acadêmica de Gestão e Tecnologia da Informação (DIATINF) Campus Natal-Central

**RESUMO:** Este artigo descreve as principais características do Routing Information Protocol (RIP) em suas duas versões e esclarece quais deficiências da versão 1 foram solucionadas na versão 2 deste protocolo. São realizadas análises, por meio de um estudo de caso considerando eventos reais, levando em consideração o aspecto de segurança, tratado na versão 2 através do recurso de autenticação. Os resultados do experimento comprovaram a eficácia do recurso, prevenindo a infraestrutura da rede contra ataques de blackhole e negação de serviço.

**PALAVRAS-CHAVE:** Protocolos de roteamento, RIPv2, segurança, autenticação.

**ABSTRACT:** This paper describes the main characteristics of the Routing Information Protocol (RIP) in its two versions, highlighting the improvements made in the version 2 of this

protocol. Analyses are performed by means of a case study considering real events, taking into account the security aspect, treated in the version 2 by the authentication feature. The results of the experiment proved the effectiveness of the improvements, being able to preventing the network infrastructure from blackhole and denial of service attacks.

**KEYWORDS:** Routing protocols, RIPv2, security, authentication.

### 1 | INTRODUÇÃO

A Internet, vista hoje como o principal meio de comunicação da atualidade, cujo número de usuários ultrapassa três bilhões (Internet Live Stats, 2015), é responsável por interconectar milhares de redes distribuídas ao redor do mundo, viabilizando a comunicação até mesmo nas áreas mais remotas.

Em consequência do vertiginoso crescimento da rede nas últimas décadas, uma série de adaptações foram requeridas para possibilitar um melhor desempenho, tais como o aprimoramento do sistema de roteamento e a divisão das redes em regiões administrativas, denominadas Sistemas Autônomos (Autonomous Systems – AS), que correspondem a áreas onde os roteadores conhecem detalhadamente a estrutura da rede

em que está inserido (Vetriselvan et al, 2014).

O RIP (Routing Information Protocol), é um protocolo de roteamento IGP (Interior Gateway Protocol) (RFC 1058), definido em 1988, que utiliza o algoritmo vetor-distância e, através de anúncios trocados entre os roteadores, define o caminho para uma rede usando como métrica a contagem de saltos, que é o número de redes que um pacote atravessa até alcançar o destino (Vetriselvan et al, 2014).

Com o advento do endereçamento IP sem classes (Classless Inter-Domain Routing – CIDR) (RFC 1519), onde as máscaras de sub-rede se tornaram flexíveis, e de protocolos de roteamento IGP mais elaborados (como o OSPF, definido no RFC 2328) o RIP, em sua versão original, pareceu se tornar obsoleto.

No entanto, a sua facilidade de configuração e manutenção, além da boa performance em ASs pouco numerosos, resultou em esforços da comunidade científica para adaptar o protocolo às exigentes necessidades dos usuários e serviços da Internet (Wang, 2001), sendo definida a versão 2 em 1994 (RFC 2453). Essa atualização manteve o algoritmo vetor-distância e trouxe novas características, como adaptação ao CIDR, autenticação, endereço de next-hop, etiquetas de rota e multicasting (RFC 1721), ao mesmo tempo que manteve sua simplicidade, tornando o RIP um dos protocolos de roteamento IGP mais empregados em redes de pequeno-médio porte da atualidade (Mueller, 2006).

Neste contexto, este trabalho pretende investigar o impacto das contribuições fornecidas ao sistema de roteamento Internet por meio das adaptações providas através do advento do RIPv2. Por questões de limitação de espaço, será apresentado um breve estudo dos principais atributos e aplicabilidades do protocolo, com ênfase no aspecto de segurança, tratado no RIPv2 através do recurso de autenticação. Para isso será apresentado um estudo de caso fazendo uso de simulações, no Graphical Network Simulator-3 (GNS3), considerando eventos baseados em situações reais que comprovem a eficácia deste recurso.

O restante deste artigo está organizado da seguinte maneira: A seção 2 realiza uma revisão, apresentando o comparativo entre as duas versões do protocolo RIP. A seção 3 é dedicada ao estudo de caso, apresentando análises por meio de simulações. Por fim, a seção 4 apresenta as considerações finais e faz apontamentos de trabalhos futuros.

## **2 | REVISÃO BIBLIOGRÁFICA**

Esta seção apresenta em detalhes as características e o funcionamento do protocolo RIP, elucidando as principais diferenças entre as versões 1 e 2.

## 2.1 Conceitos Básicos Do Protocolo RIP

O RIP possui a tarefa de descobrir a melhor rota de acordo com a métrica da menor contagem de saltos, fazendo uso do algoritmo de vetor de distância (Distance Vector), através de trocas periódicas de tabelas de roteamento entre roteadores presentes no AS (RFC 1058). Este algoritmo é o atributo de base do RIP, inalterado em ambas versões.

As extensões providas através do RIPv2 permitem que os roteadores compartilhem informações adicionais, não sendo este exatamente um novo protocolo (RFC 1721). A Figura 1 apresenta a estrutura genérica de uma mensagem RIPv2.

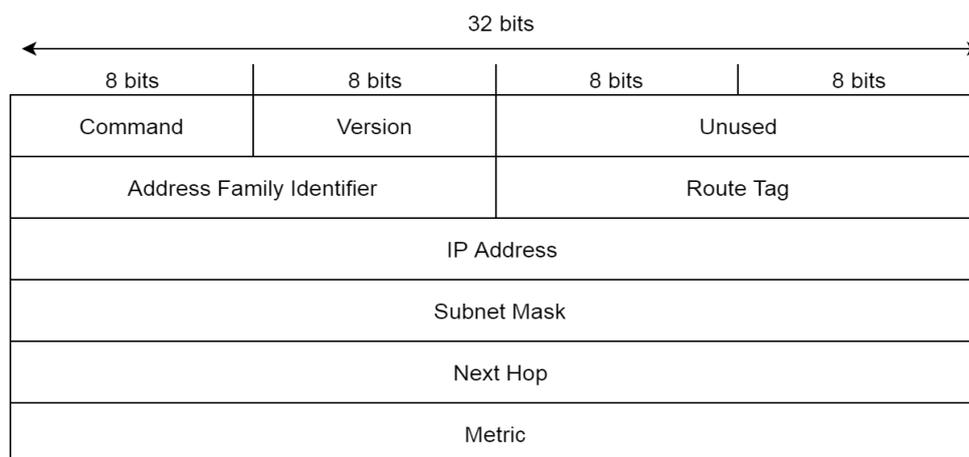


Figura 1: Estrutura de uma mensagem RIPv2 (RFC 1723).

As duas versões do RIP compartilham campos em comum: Command identifica o pacote como uma consulta ou uma resposta do roteador solicitado; Version define a versão utilizada; O Identificador de Família de Endereços (campo Address Family Identifier – AFI) especifica o tipo de endereço que é utilizado, sendo o valor para IP igual a 2; IP Address é um endereço IPv4 habitual com 4 octetos (RFC 1058); Metric contém a contagem de saltos para alcançar o destino. Em ambas versões, valores maiores que 15 saltos indicam que uma rota é considerada inalcançável.

A versão 2 traz o campo Next Hop, que otimiza rotas em ASs que utilizam múltiplos IGP (RFC 1721). O campo Route tag é utilizado para propagar rotas externas à um AS (RFC 1721).

## 2.2 Características Do RIPv2

### 2.2.1 Autenticação

Ao mesmo tempo que a Internet crescia em proporções quase imensuráveis, exigindo por parte dos projetistas novos mecanismos que a mantivesse em funcionamento, vários problemas de segurança surgiam a cada dia, demandando a criação de estratégias que garantissem também a confidencialidade e integridade das informações (Papadimitratos & Haas, 2002). Como exemplo desta imprescindibilidade

por segurança está a necessidade de prevenir a propagação de rotas falsas pelo AS (RFC 1722), característica que foi incorporada pelo RIPv2. A Figura 2 apresenta o formato de uma mensagem RIPv2 fazendo uso do recurso de autenticação.

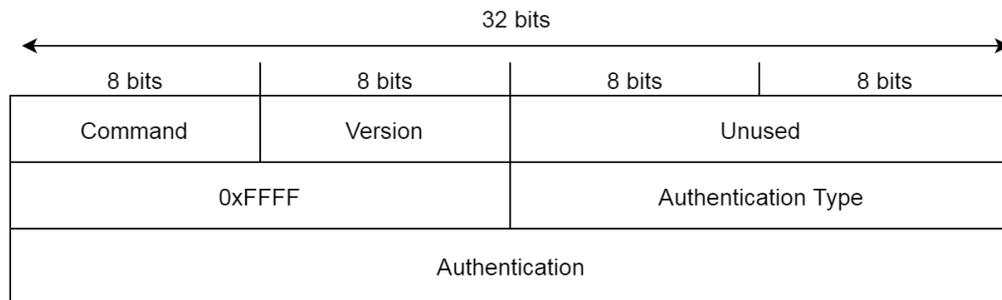


Figura 2: Cabeçalho de uma mensagem RIPv2 fazendo uso da autenticação (RFC 1723)

A partir do Identificador de Família de Endereços (AFI), definido como 0xFFFF, os campos Authentication Type e Authentication definem o tipo de autenticação e a senha utilizada, respectivamente (RFC 1723).

Roteadores não configurados com autenticação são capazes de receberem anúncios de roteadores sem autenticação e de roteadores com RIPv1. Caso contrário, as mensagens são descartadas. O recíproco também ocorre: roteadores configurados com autenticação apenas são capazes de receberem anúncios de roteadores aprovados no teste de autenticação. Caso contrário, as mensagens também serão descartadas. Por razões de segurança, roteadores com o recurso de autenticação habilitado jamais receberão anúncios de roteadores com RIPv1 (RFC 1723).

Caso a primeira entrada na mensagem AFI contenha o valor 0xFFFF, o restante da mensagem conterá a informação da autenticação, e assim os roteadores com RIPv1 descartarão a este recurso. No entanto, isto não impede que esse roteador visualize os anúncios de um roteador com RIPv2. Quando se desejar que isso seja evitado, o RIPv2 pode utilizar endereços multicast (RFC 1723).

### 2.2.2 Multicasting

Um endereço multicast pode ser utilizado no lugar do endereço broadcast para requisitos de anúncios. Isso faz com que os anúncios sejam destinados apenas para roteadores com RIPv2. Além de evitar que outros roteadores recebam as mensagens, o multicasting reduz carga na rede.

Este é um atributo configurável, a fim de manter compatibilidade com a versão anterior. A configuração é feita para cada interface desejada (RFC 1723).

### 2.2.3 Etiquetas de rota

A etiqueta de rota, definido no campo Route Tag, provê um método para diferenciar rotas geradas pelo protocolo RIP de rotas geradas por um protocolo externo ao AS

(RFC 1723).

#### 2.2.4 Máscara de sub-rede

O grande estímulo da comunidade científica em desenvolver uma nova versão para o RIP foi a necessidade de adaptação às novas máscaras de sub-rede de tamanho variável, definidos no CIDR (RFC 1519). Este campo contém 32-bits, sendo sucedido do endereço IP. Assim, o RIP pode ser implementado em ASs que precisam de informações precisas sobre sub-redes, facilitando o encaminhamento das mensagens (RFC 1722).

#### 2.2.5 Próximo salto

Os endereços de próximo salto (next hop) foram adicionados para que haja uma maior eficiência no roteamento de um pacote. Se definido como 0.0.0.0, o roteador utilizará como gateway o roteador que foi origem dos anúncios. Se este roteador conhecer uma rota melhor para uma rede de destino, o que pode ocorrer se estiver com outro IGP funcionando, este campo é utilizado para especificar outro next hop que não seja ele mesmo (RFC 1723).

### 3 | SIMULAÇÕES E ANÁLISE

Basicamente, a segurança da Internet depende de quatro níveis básicos de proteção: (i) proteção para o sistema final; (ii) proteção para comunicação fim-a-fim; (iii) proteção para a Qualidade de Serviço (QoS) e; (iv) proteção para a infraestrutura de rede. Em se tratando da infraestrutura da rede, podem haver ataques aos roteadores, comprometendo o funcionamento de diferentes maneiras, uma vez que a conectividade de um AS está diretamente relacionada ao correto funcionamento do sistema de roteamento (Pescapè, 2005).

Ataques à roteadores podem ter duas origens: externa e interna. Os ataques externos são associados à roteadores pseudo-legítimos que injetam informações falsas na rede. Ataques internos são realizados a partir de um ou mais roteadores comprometidos já existentes no AS. Diferentes tipos de ações podem ser realizados durante ataques a roteadores, tais como a Interrupção de Rotas (*Route Disruption*), Negação de Serviço (*Denial of Service - DoS*) (Kapur & Khatri, 2015) e até mesmo ataques de *Blackhole* (Alves Júnior & Albin, 2012). No ataque do tipo *blackhole*, por exemplo, um roteador malicioso pode propagar um caminho inexistente para uma rede, fazendo com que o roteador alvo receba as mensagens e as descarte, causando a interrupção da comunicação entre duas ou mais redes (Pescapè, 2005).

O cenário apresentado na Figura 3 simula parte de um AS, onde os roteadores (R1, R2 e R3) compartilham anúncios das redes conhecidas, de modo que as redes remotas (Rede A e Rede B) sejam capazes de se comunicar. Um roteador intruso (R4)

é conectado à Rede A com objetivo de desferir um ataque *blackhole*. Em condições normais, as mensagens trocadas entre as duas redes (A e B) devem atravessar os enlaces intermediários.

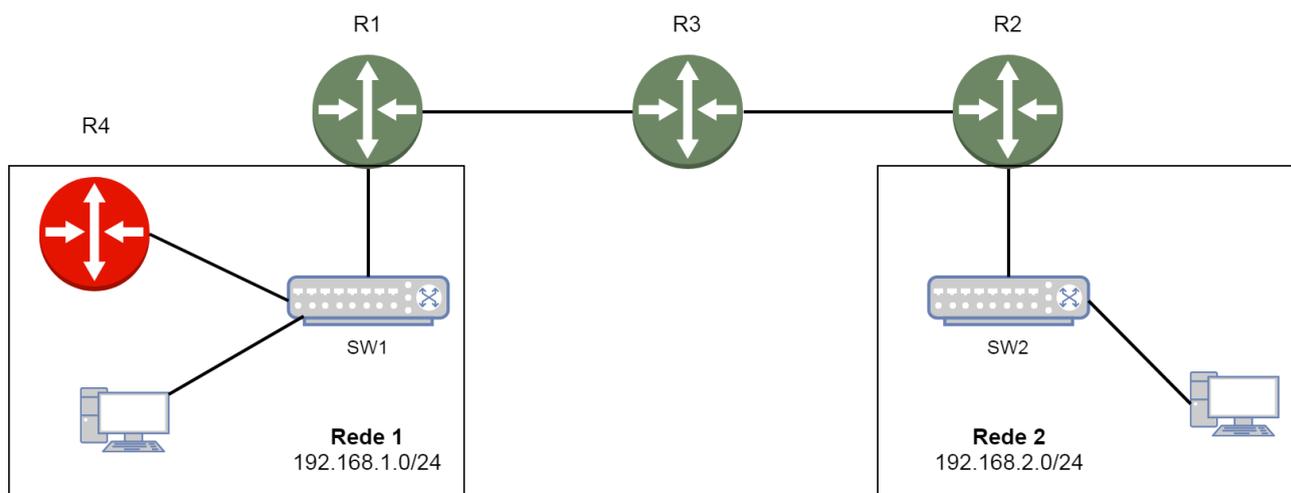


Figura 3: Topologia do estudo de caso.

A Figura 4 exibe o resultado de um traceroute enviado do host PC1 para o host PC2, detalhando a rota percorrida pelos pacotes, da origem até o destino, a saber: R1 (salto 1), R3 (salto 2), R2 (salto 3) e finalmente o host PC2 (salto 4).

```
PC1> trace 192.168.2.11 -P 1
trace to 192.168.2.11, 8 hops max (ICMP), press Ctrl+C to stop
 1  192.168.1.1  15.626 ms  15.623 ms  15.623 ms
 2  10.0.0.2   91.253 ms  46.876 ms  56.248 ms
 3  10.0.0.6   93.756 ms  46.977 ms  76.089 ms
 4  192.168.2.11 78.128 ms  94.167 ms  78.129 ms
```

Figura 4: Rota entre PC1 e PC2.

Assim que o roteador R4 é anexado à topologia, os anúncios maliciosos alcançam o roteador R1, como mostra a Figura 5. As informações enviadas através do anúncio malicioso serão indexadas à tabela de roteamento de R1.

```
RIP: received v2 update from 192.162.1.2 on FastEthernet0/0
192.168.2.0/24 via 0.0.0.0 in 1 hops
```

Figura 5: Atualização da tabela de roteamento em R1.

A partir desse momento, todos os pacotes com destino à Rede B serão encaminhados ao roteador R4, que simplesmente os descartará, fazendo com que a comunicação legítima não ocorra. A Figura 6 mostra o resultado de um novo traceroute enviado do host PC1 para o host PC2 após o ataque ao roteador R1, constatando a

eficácia do ataque.

```
PC1> trace 192.168.2.11 -P 1
trace to 192.168.2.11, 8 hops max (ICMP), press Ctrl+C to stop
 1  192.168.1.1  15.627 ms  15.627 ms  15.632 ms
 2  Redirect Network, gateway 192.168.1.1 -> 192.168.1.2
 1  192.168.1.2  15.625 ms  15.628 ms  15.628 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
```

Figura 6: Falha no teste de conectividade com a Rede B.

Situações como esta podem ser evitadas fazendo o uso da ferramenta de autenticação do RIPv2. A configuração da autenticação nos roteadores é feita utilizando um chaveiro e uma série de chaves definidas através de linhas de comando, em cada roteador (Li et al. 2012). No cenário apresentado neste estudo de caso foi configurado um chaveiro com uma única chave, que deve ser a mesma em todos os roteadores, possibilitando a troca de informações.

Quando os chaveiros e as chaves são configurados, é necessário que a autenticação seja habilitada em cada interface, explicitando o tipo (texto claro ou criptografado) (Li et al. 2012). Feito isso, o roteador envia, por esta interface, uma mensagem Request, solicitando a tabela de repasse do roteador vizinho, conforme exibido na Figura 7.

```
Routing Information Protocol
  Command: Request (1)
  version: RIPv2 (2)
  Authentication: simple Password
  Authentication type: simple Password (2)
  Password: RIP
  Address not specified, metric: 16
```

Figura 7: Mensagem de requisição enviada para R2.

O formato da mensagem RIP é semelhante ao apresentado na Figura 2. O primeiro byte (com valor 1) identifica a mensagem de requisição. O tipo de autenticação é definido como senha simples, com valor numérico igual a 2, seguido pela senha em texto claro (“RIP”). O restante da mensagem especifica o tipo da resposta solicitada. Neste caso, o anúncio vazio e a métrica de valor igual a 16 explicita que toda a tabela de roteamento está sendo requerida (RFC 2453). Ao receber este pacote, o roteador R3 responde com o anúncio da sua tabela de roteamento. A Figura 8 apresenta o resultado do comando debug ip rip, no console do roteador R1, confirmando estas operações.

```
RIP: received packet with text authentication RIP
RIP: received v2 update from 10.0.0.2 on Serial2/0
10.0.0.4/30 via 0.0.0.0 in 1 hops
192.168.2.0/24 via 0.0.0.0 in 2 hops
```

Figura 8: Recepção do anúncio do roteador R2 no roteador R1.

Após estas modificações, o roteador malicioso R4 não será capaz de operar com os outros roteadores, inviabilizando o ataque. Neste caso, os anúncios continuarão a ser enviados, mas serão rejeitados pelo roteador R1, como mostra a Figura 9.

```
RIP: ignored v2 packet from 192.168.1.2 (invalid authentication)
```

Figura 9: Rejeição ao anúncio malicioso do roteador R4.

A autenticação pode se tornar mais eficiente caso seja criptografada. Se assim for desejado, deverá ser especificado este tipo de autenticação nas interfaces de um roteador. O RIPv2 utiliza o algoritmo de criptografia MD5, definido para o RIP em 1997 (RFC 2082). Quando uma interface está utilizando esse método criptográfico, os campos de autenticação da mensagem passam a conter informações adicionais, como identificador de chave, tamanho dos dados de autenticação e número de sequência (caso o tamanho dos dados de autenticação ultrapasse 24 bytes). A Figura 10 apresenta o mesmo anúncio gerado pelo roteador R3, mas com criptografia habilitada.

```
Routing Information Protocol
  Command: Response (2)
  Version: RIPv2 (2)
  Authentication: Keyed message Digest
    Authentication type: Keyed Message Digest (3)
    Digest Offset: 64
    Key ID: 1
    Auth Data Len: 20
    Seq num: 1
    Zero Padding
  Authentication Data Trailer
    Authentication Data: 6f 90 07 67 e5 b2 92 7e 12 8e 41 e8 46 83 08 2d
  IP Address: 10.0.0.4, Metric: 1
  IP Address: 192.168.2.0, metric: 2
```

Figura 10: Anúncio com autenticação criptografada.

Como mostrado na Figura 10, os dados de autenticação não são mais apresentados em texto claro, sendo precedidos pelas informações adicionais citadas anteriormente e imediatamente sucedidos pelo anúncio.

## 4 | CONCLUSÃO

Este trabalho analisou as notáveis contribuições do RIPv2 para a o sistema de roteamento, principalmente no aspecto de segurança. As simulações permitiram

uma maior acurácia na análise do envio e recebimento dos pacotes de autenticação, fornecendo um maior entendimento dos seus formatos, além de comprovar a eficiência contra ataques do tipo blackhole e, conseqüentemente, de Negação de Serviço, evitando assim o comprometimento do funcionamento da rede. Como trabalhos futuros, pretende-se realizar novos estudos para avaliar as demais extensões do RIPv2 em termos de performance, para os recursos de multicasting, next hop e route tags.

## REFERÊNCIAS

Alves Júnior, J., Albin, L.C.P., “**Um Protocolo de Roteamento Resistente a Ataques Blackhole sem detecção de nós maliciosos**”. XXX Simpósio Brasileiro de Telecomunicações (SBrT'12). Setembro 2012.

Cisco Troubleshooting TechNotes. “**Redistributing Routing Protocols**”, 2012, Disponível em: <http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html>. Acesso em 22/08/2015.

Internet Live Stats. “**Internet Usage & Social Media Statistics**”, Disponível em: <http://www.internetlivestats.com>. Data de acesso: 25/09/2015.

Kapur, R.K.; Khatri, S.K., “**Analysis of attacks on routing protocols in MANETs**” in Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in , vol., no., pp.791-798, 19-20 March 2015.

Li, Xiaohua; Zhao, Xiangang; Xu, Jian; Yao, Shan; Wang, Huaiwei; Zhang, Yan, “**Simulation and analysis of RIPv2 routing authentication based on GNS**,” in Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on , vol., no., pp.1842-1845, 3-5 March 2012.

RFC 1058. Hendrik, C. “**Routing Information Protocol**”, RFC1058, Junho, 1988. Disponível em: <https://tools.ietf.org/html/rfc1058>. Acesso em 15/08/2015.

RFC 1721. Malkin, G. “**RIP Version 2 Protocol Analysis**”, RFC1721, Novembro, 1994. Disponível em: <https://tools.ietf.org/html/rfc1721>. Acesso em 14/08/2015.

RFC 1722. Malkin, G. “**RIP Version 2 Protocol Applicability Statement**”, RFC1722, Novembro, 1994. Disponível em: <https://tools.ietf.org/html/rfc1722>. Acesso em 14/08/2015.

RFC 1723. Malkin, G. “**RIP Version 2 – Carrying Additional Information**”, RFC1723, Novembro, 1994. Disponível em: <https://tools.ietf.org/html/rfc1723>. Acesso em 15/08/2015.

RFC 2453. Malkin, G. “**RIP Version**”, RFC2453, Novembro, 1998. Disponível em: <https://tools.ietf.org/html/rfc2453>. Acesso em 29/09/2015.

Mueller, S., Ogletree, T. W, Soper, M. E. “**Upgrading and Repairing Networks**”. 5th Edition. Que, 2006.

Papadimitratos, P.; Haas, Z.J., “**Securing the Internet routing infrastructure**,” in Communications Magazine, IEEE, vol.40, no.10, pp.60-68, Oct 2002.

Pescapè, A; Ventre, G., “**Experimental analysis of attacks against intradomain routing protocols**”,

Journal of Computer Security 13, 2005.

Vetriselvan, V.; Patil, Pravin R.; Mahendran, “**M. Survey on the RIP, OSPF, EIGRP routing protocols**”. IJCSIT International Journal of Computer Science and Information Technologies, v. 5, n. 2, p. 1058-1065, 2014.

Wang, Z. “**Internet QoS, Architectures and Mechanisms for Quality of Service**”. Morgan Kaufmann Publishers, 2001

## **SOBRE OS ORGANIZADORES**

**Jorge González Aguilera:** Engenheiro Agrônomo (Instituto Superior de Ciências Agrícolas de Bayamo (ISCA-B) hoje Universidad de Granma (UG)), Especialista em Biotecnologia pela Universidad de Oriente (UO), CUBA (2002), Mestre em Fitotecnia (UFV/2007) e Doutorado em Genética e Melhoramento (UFV/2011). Atualmente, é professor visitante na Universidade Federal de Mato Grosso do Sul (UFMS) no Campus Chapadão do Sul. Têm experiência na área de melhoramento de plantas e aplicação de campos magnéticos na agricultura, com especialização em Biotecnologia Vegetal, atuando principalmente nos seguintes temas: pre-melhoramento, fitotecnia e cultivo de hortaliças, estudo de fontes de resistência para estres abiótico e biótico, marcadores moleculares, associação de características e adaptação e obtenção de vitroplantas. Tem experiência na multiplicação “on farm” de insumos biológicos (fungos em suporte sólido; Trichoderma, Beauveria e Metharrizum, assim como bactérias em suporte líquido) para o controle de doenças e insetos nas lavouras, principalmente de soja, milho e feijão. E-mail para contato: [jorge.aguilera@ufms.br](mailto:jorge.aguilera@ufms.br)

**Alan Mario Zuffo:** Engenheiro Agrônomo (Universidade do Estado de Mato Grosso – UNEMAT/2010), Mestre em Agronomia – Produção Vegetal (Universidade Federal do Piauí – UFPI/2013), Doutor em Agronomia – Produção Vegetal (Universidade Federal de Lavras – UFLA/2016). Atualmente, é professor visitante na Universidade Federal do Mato Grosso do Sul – UFMS no Campus Chapadão do Sul. Tem experiência na área de Agronomia – Agricultura, com ênfase em fisiologia das plantas cultivadas e manejo da fertilidade do solo, atuando principalmente nas culturas de soja, milho, feijão, arroz, milheto, sorgo, plantas de cobertura e integração lavoura pecuária. E-mail para contato: [alan\\_zuffo@hotmail.com](mailto:alan_zuffo@hotmail.com)

Agência Brasileira do ISBN  
ISBN 978-85-7247-474-0

