Investigação e Avaliação do Impacto da Aplicação de Mecanismos de Segurança em *Voice over Internet Protocol* (VoIP)

Rafael Mendes Pereira
Liane M. R. Tarouco

Roteiro

- Introdução
- Riscos
- Soluções
- Impacto
- Avaliação
- Proposta
- Referências

Introdução

- Voz sobre IP (VoIP):
  - Novos recursos (compartilhamento de dados);
  - Maior flexibilidade e menor custo em relação à comunicação convencional.
- Apresenta novas vulnerabilidades;
- Várias soluções existentes para segurança (ITU-T e IETF);
- Investigação do impacto dos mecanismos de segurança.

Riscos de Segurança em VoIP

- Vulnerabilidades: Sinalização e Mídia;
- Privacidade:
  - Interceptação de chamadas e escuta indevida.
- Integridade:
  - Alteração indevida das chamadas.
- Disponibilidade do serviço:
  - Indisponibilidade ou degradação no serviço.

Soluções para Segurança

- ITU-T:
  - H.235: prover segurança para a recomendação H.323.
- IETF:
  - Sinalização:
    - Autenticação *Digest* HTTP;
    - S/MIME (*Secure* MIME).
  - Mídia:
    - SRTP (*Sercure Real-time Transport Protocol*).
- TLS (*Transport Layer Security*);
- IPsec (*Internet Protocol Security).*

Impacto

- Aplicações altamente sensíveis ao atraso:
  - 150 ms atraso máximo:
    - 1 a 30 ms codificação;
    - 100 ms transmissão (*link delay, jitter buffer, etc)*.
    - 20 ms atraso adicional.
- Fatores que afetam a QoS:
  - Expansão dos dados (Transmissão, Roteamento, Enfileiramento, *Jitter*);
  - Aumento do Processamento.

Avaliação

- Requisitos de QoS:
  - Sinalização: baixo;
  - Mídia: alto.
- Mecanismos:
  - SRTP;
  - IPsec (VPN – *Virtual Private Network*).
- Fatores:
  - Expansão dos pacotes;
  - Atraso com criptografia.

IPsec

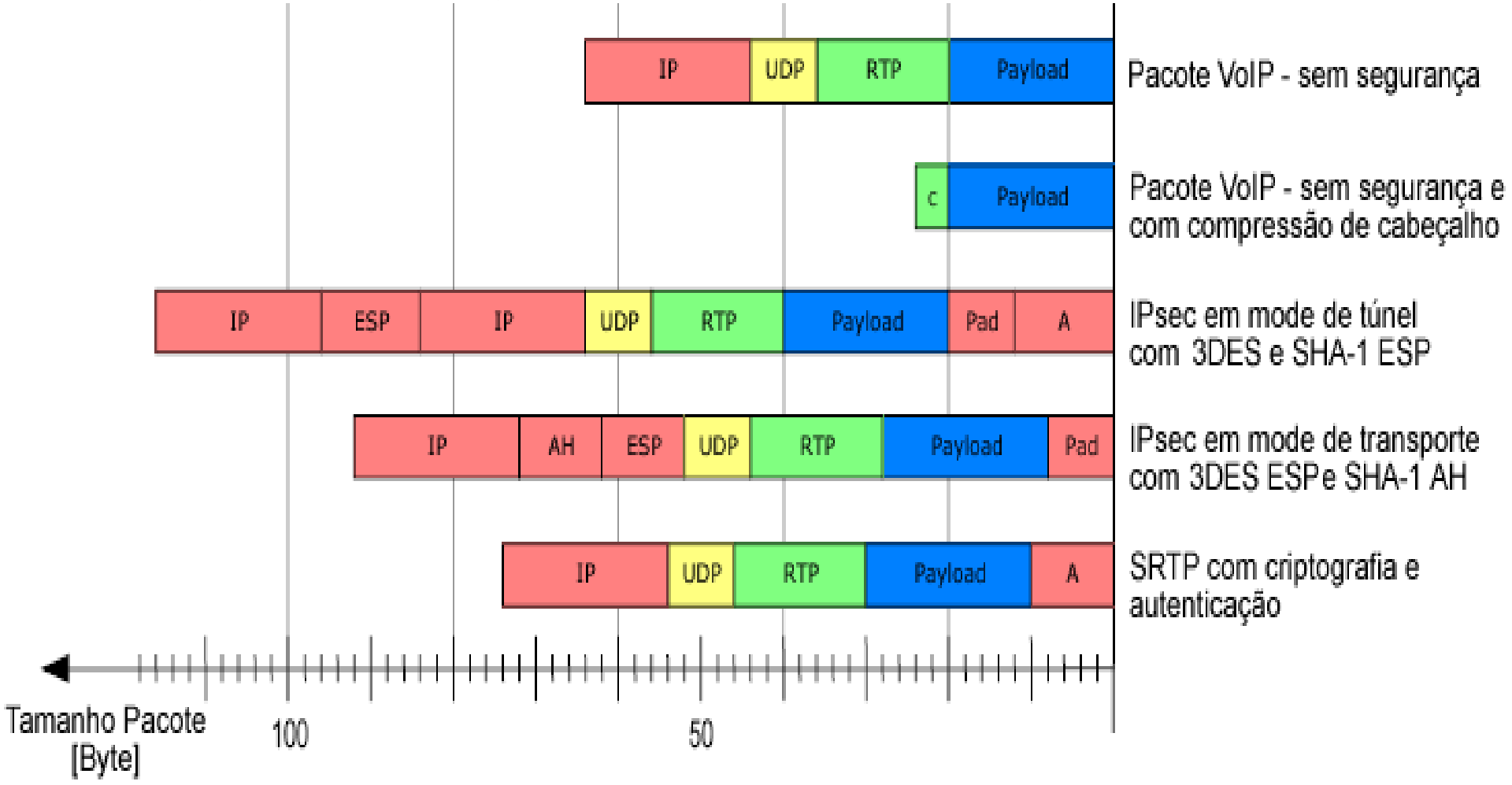
- Segurança para o protocolo IP;
- *Secuity Associantion* (SA);
- Modo:
  - Transporte;
  - Túnel.
- Cabeçalhos:
  - AH (*Authentication Header*):
    - Integridade, autenticação e anti-replay.
  - ESP (*Encapsulation Security Payload*):
    - Privacidade, integridade, autenticação e anti-replay.
- Suporte obrigatório:
  - DES (*Data Encryption Standard*);
  - HMAC (*Hashed Message Authentication Code*)
    - MD5 (*Message-Digest algorithm 5*)e SHA-1(*Secure Hash Algorithm*).

SRTP

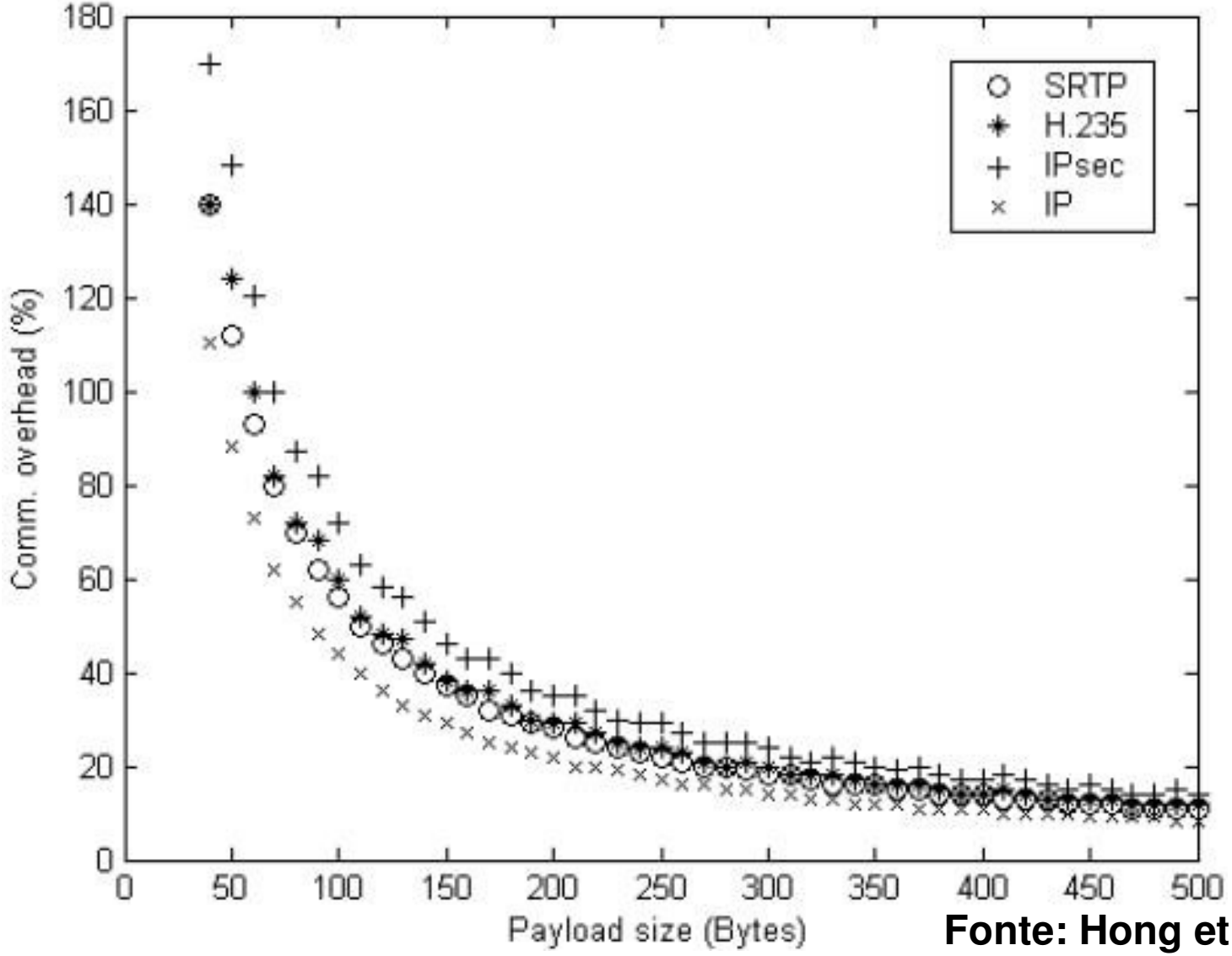
- *Framework*: Extensão opcional para segurança no protocolo RTP;
- Privacidade, integridade, autenticação e anti-replay;
- Algoritmo padrão:
  - AES / CTR (*Advanced Encryption Standard* em modo de contagem);
  - HMAC / SHA-1.

Expansão dos Dados

- *Payload*: 20 Bytes

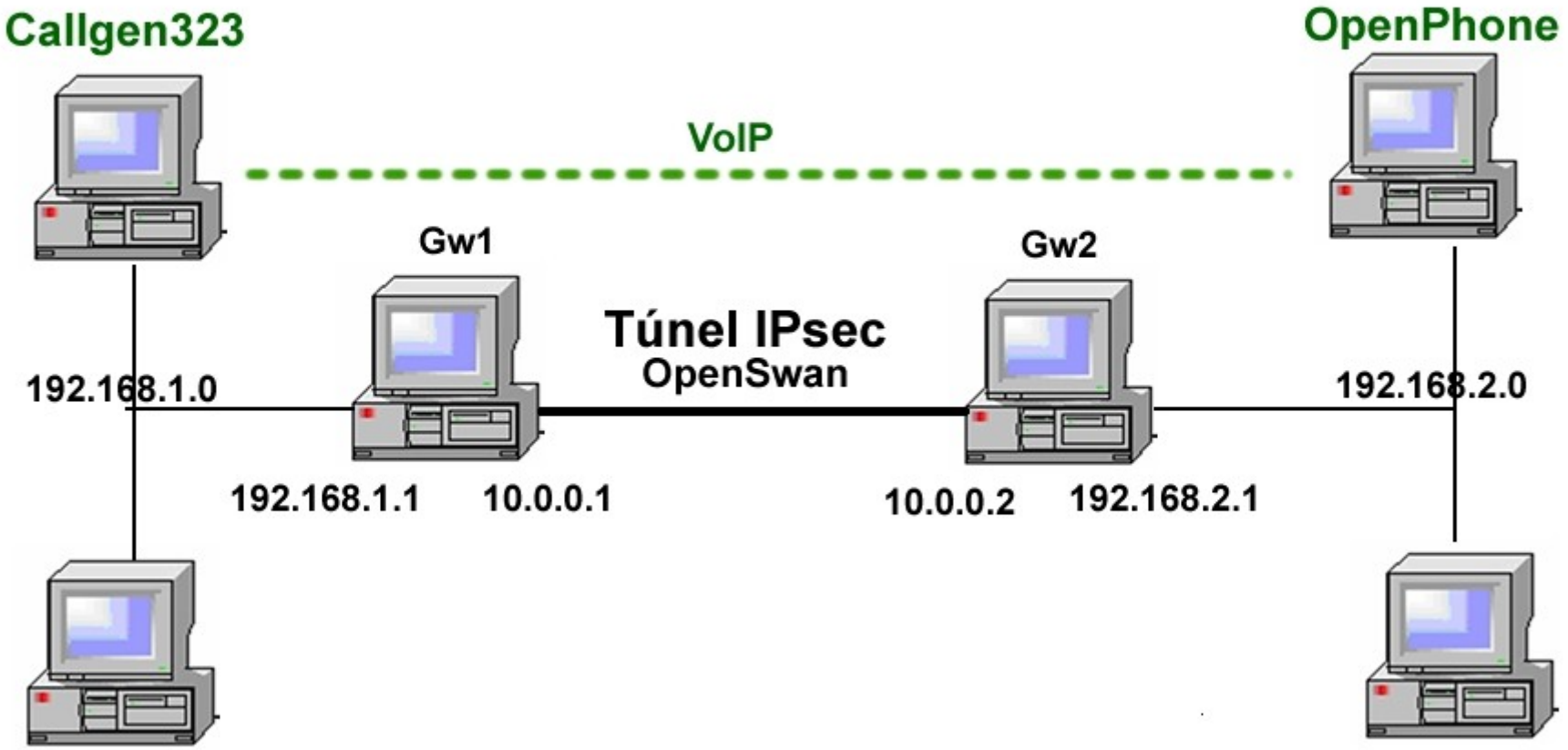


Expansão dos Dados

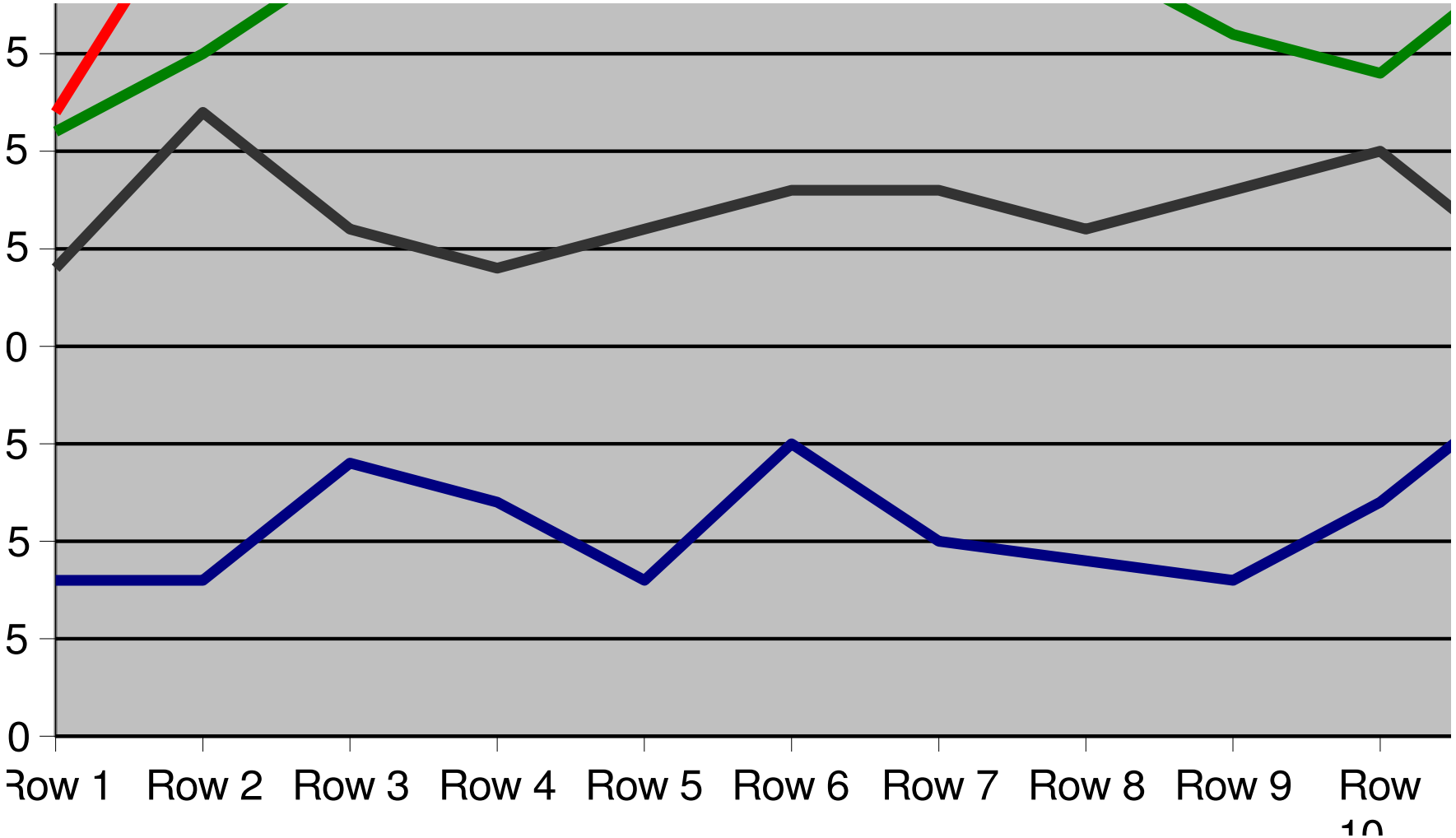


Fonte: Hong et al. (2004)

Ambiente de testes

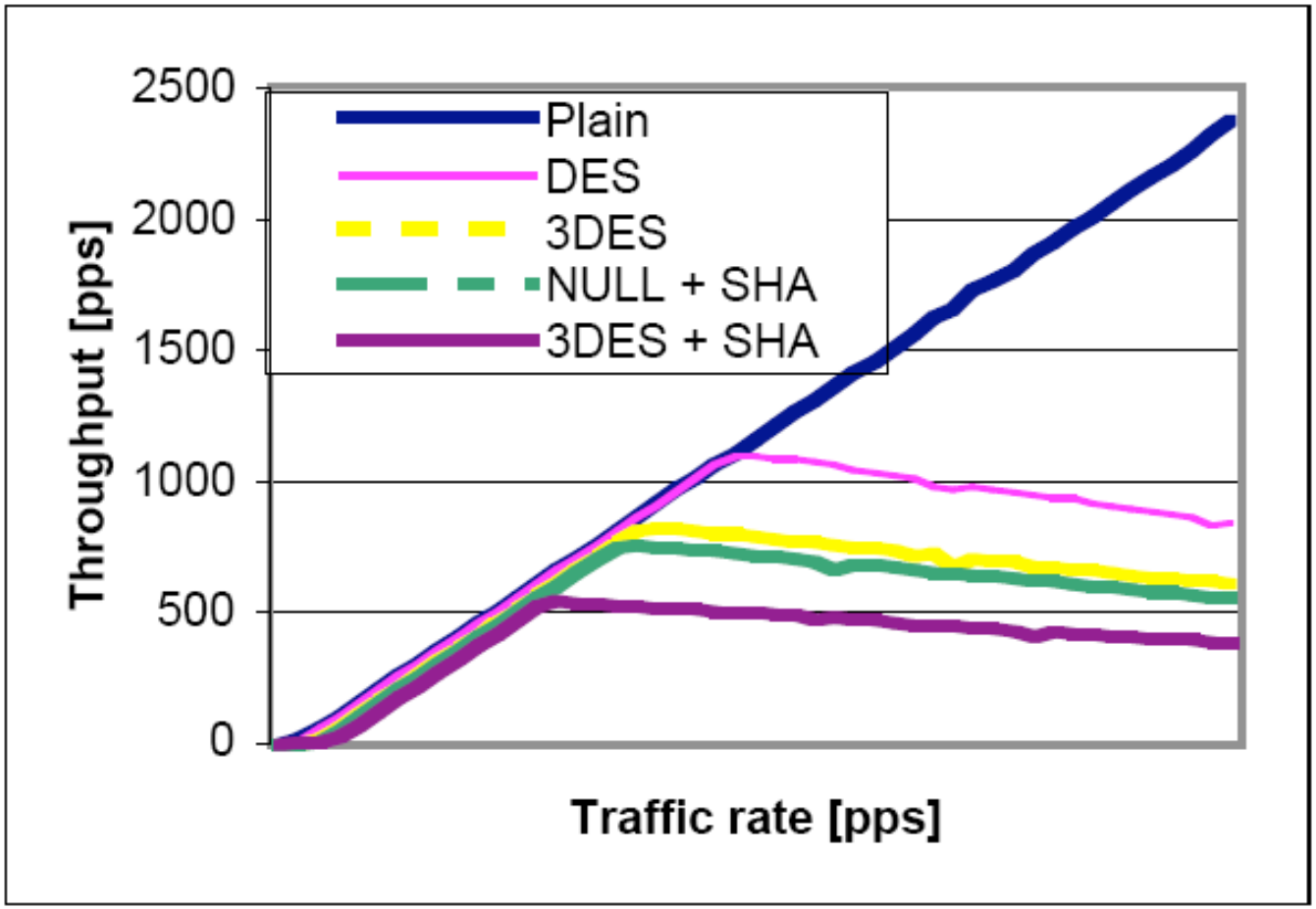


Atraso Fim-a-Fim



Throughput Criptografia

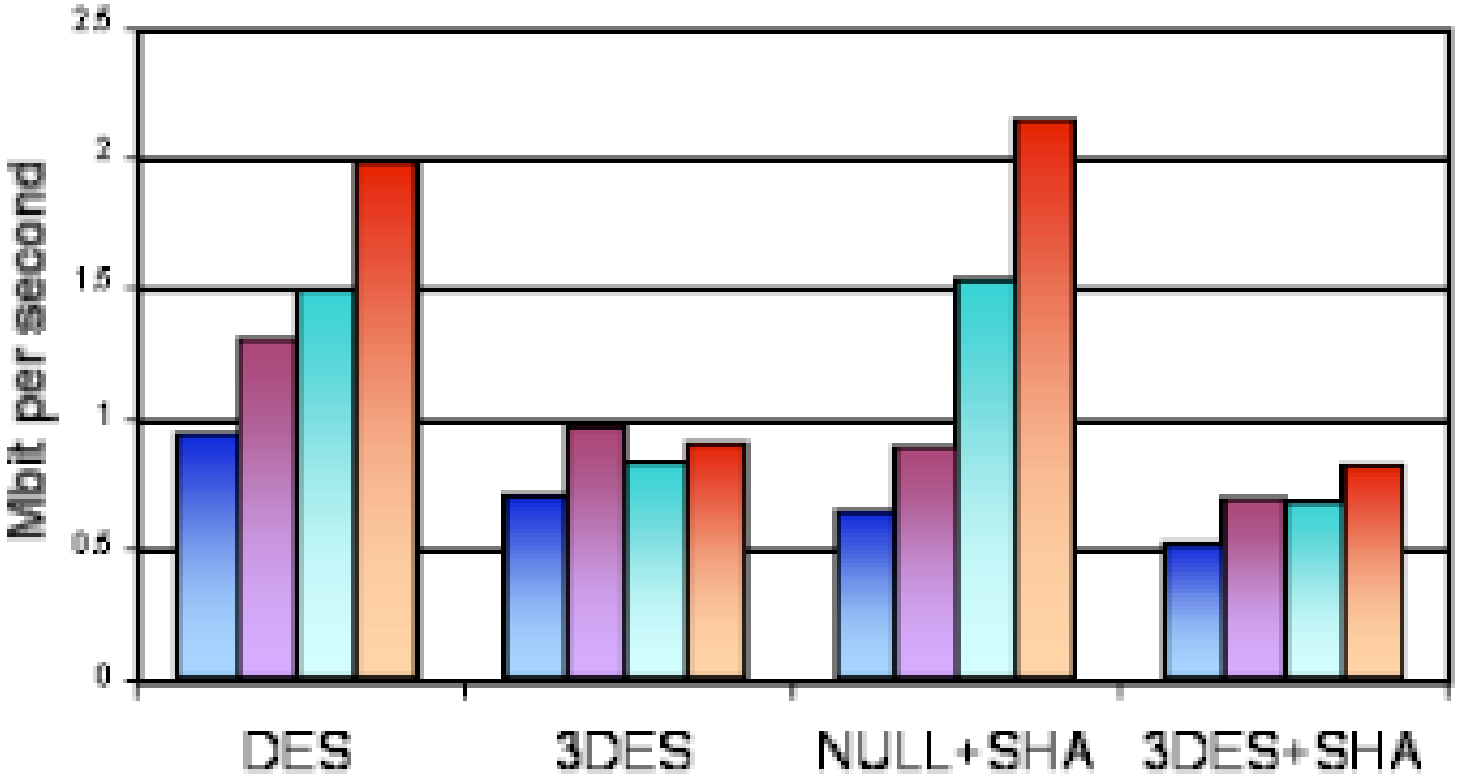
- IPsec:



Fonte: Barbieri (2002)

Throughput Criptografia

- IPsec:

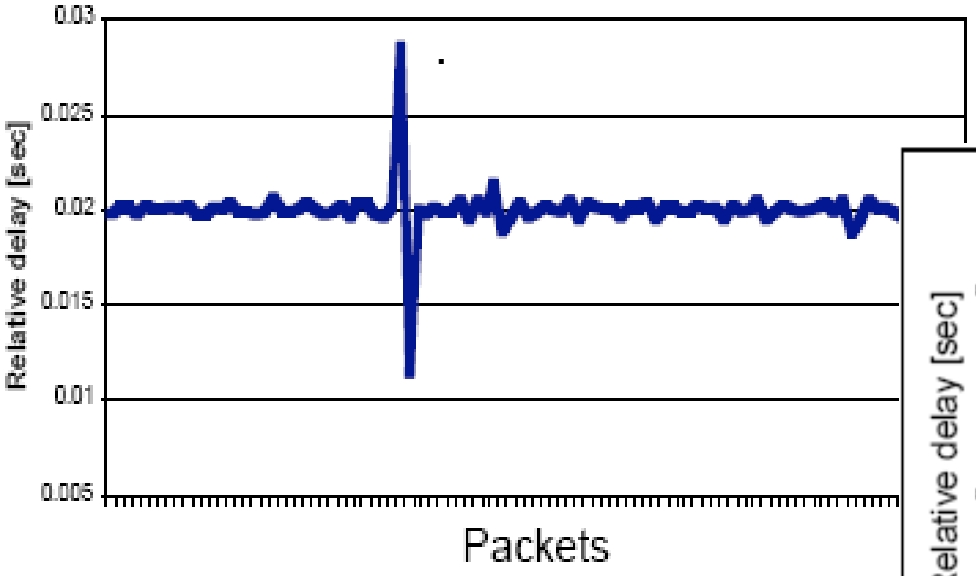


Fonte: Barbieri (2002)

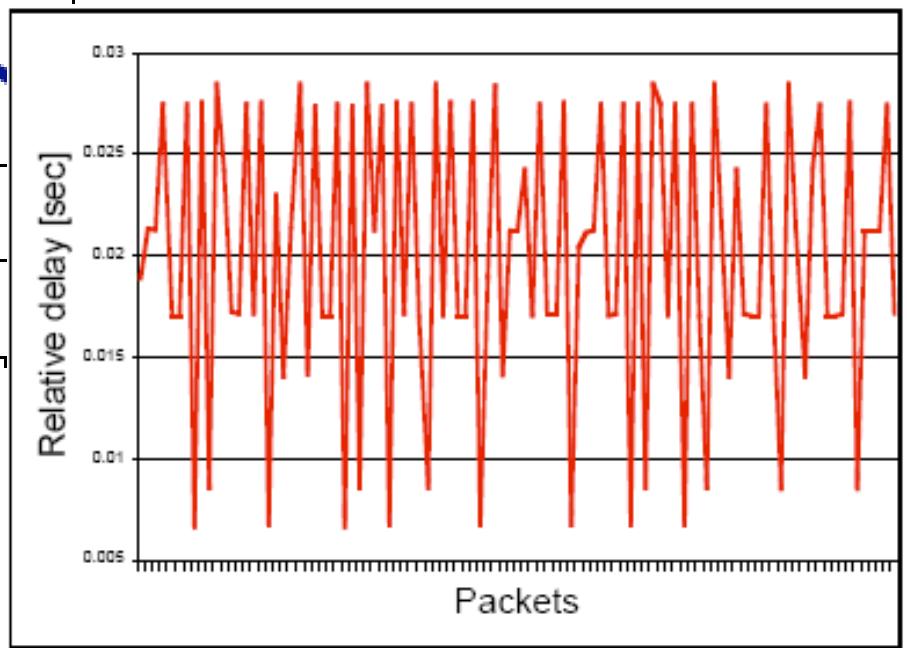
Throughput Criptografia

- IPsec: Tempo de atraso de chegada:

VoIP



VoIP + tráfego heterogêneo.



Fonte: Barbieri (2002)

Resultados

- SRTP apresenta um *framework* com baixo custo computacional e de banda, evita uma expansão grande dos pacotes e utiliza algoritmos de criptografia modernos [Baugher et al., 2004] [Hong et al., 2004] [Kuhn et al., 2005].

Problemática

- SRTP necessita alteração dos aplicativos já implantados!

- Proposta:

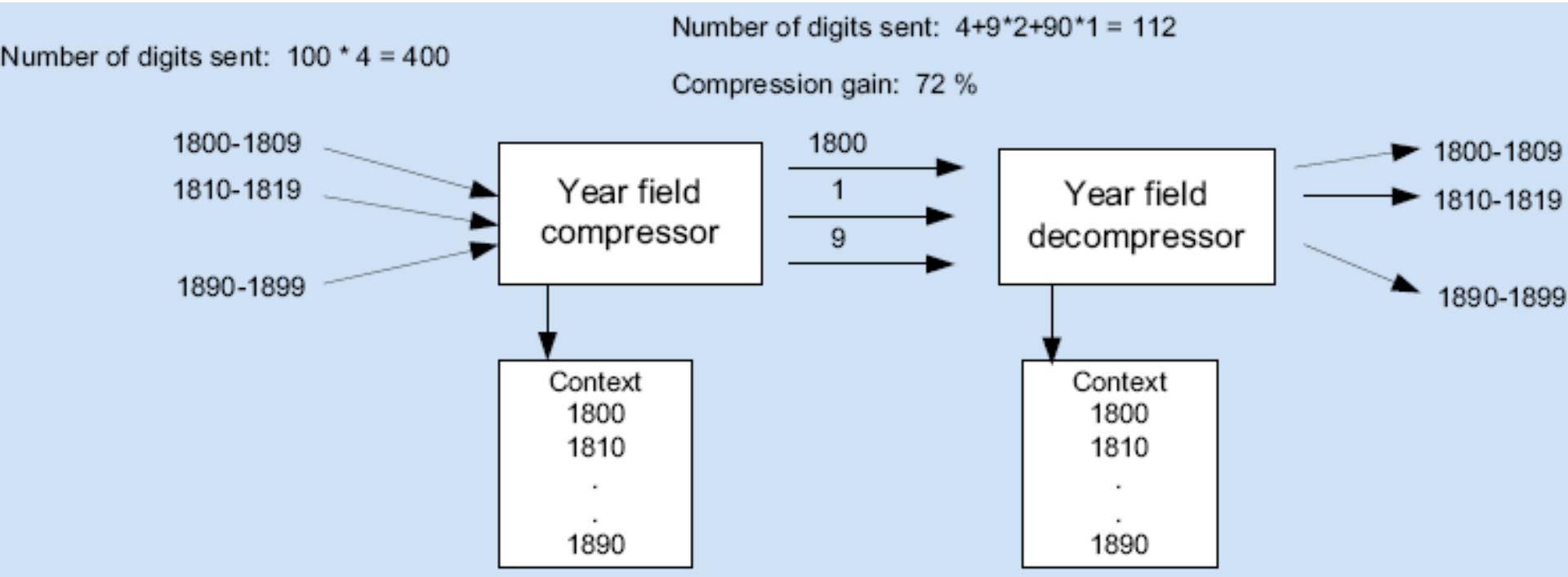
  Investigação de soluções que melhorem o desempenho do IPsec na aplicação de segurança em VoIP

Proposta – Compressão dos Dados

- ROHC (*RObust Header Compression*)
  - Compressão para os cabeçalhos:
    - RTP/UDP/IP;
    - UDP/IP;
    - ESP/IP.
  - Alcança compressão do cabeçalho para até 1 byte;
  - *Window-based Least Significant Bits encoding* (W-LSB)

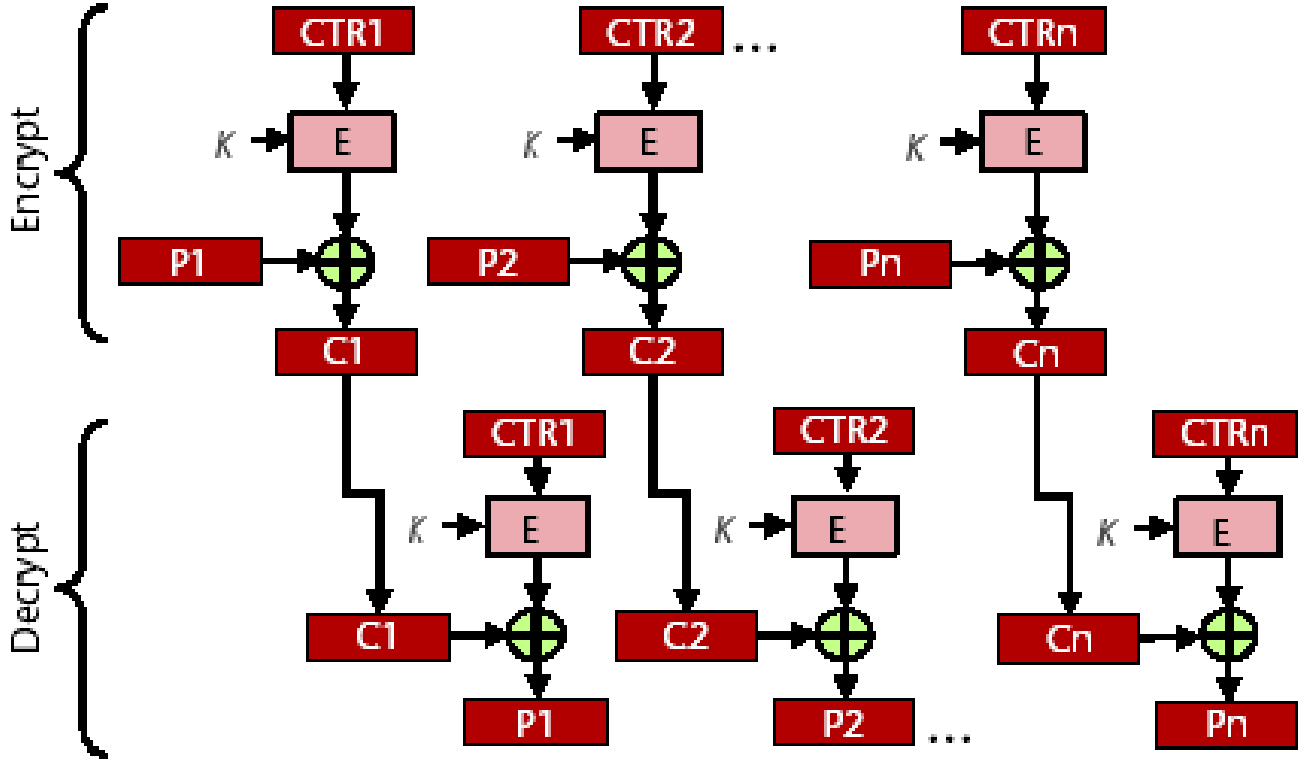
Proposta – Compressão dos Dados

- ROHC (*RObust Header Compression*)
  - (W-LSB):



Proposta – Algoritmo de Criptografia mais Rápido

- AES/CTR (*Advanced Encryption Standard/ Counter Mode*)

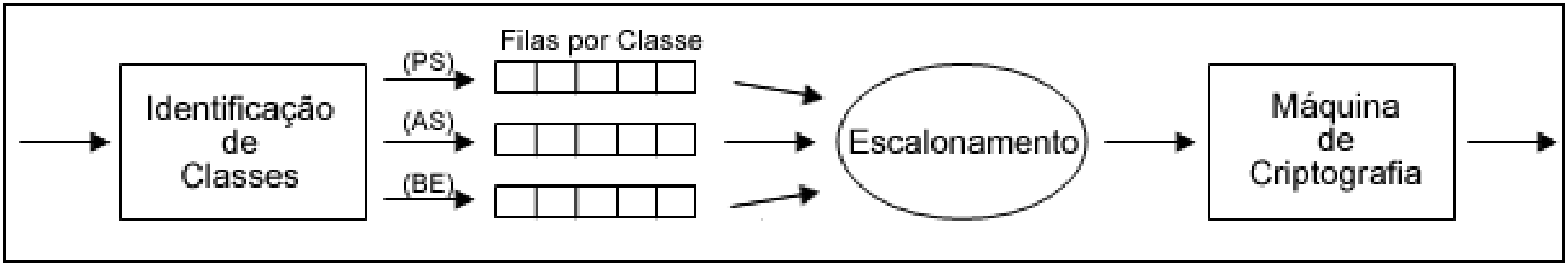


Proposta – QoS na Máquina de Criptografia

- Diminuir o descarte de pacotes na criptografia de pacotes de VoIP;
- Baseado em métodos de QoS (*DiffServ*);
- Identificação dos fluxos por meio de classes;
- Definição de prioridades por tipo de classe: maior prioridade para fluxos de tempo real.

Proposta – QoS na Máquina de Criptografia

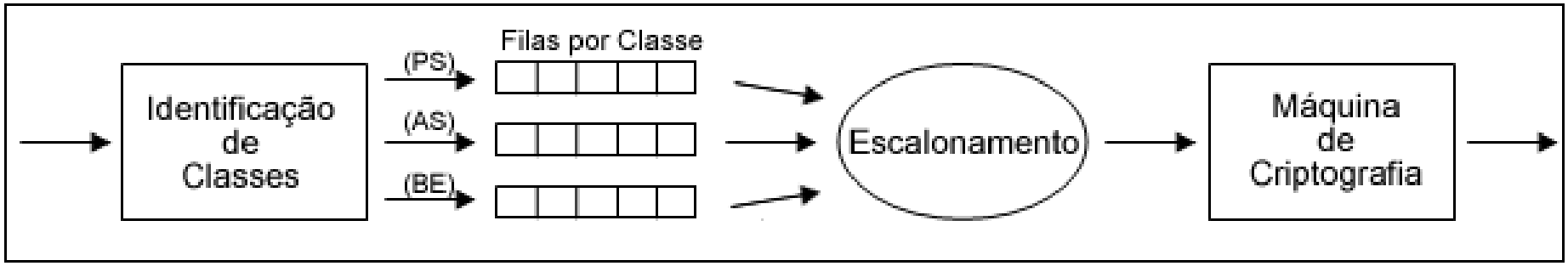
Fluxo de Dados para Criptografia



- Identificação das Classes:
  - Campo *Differentiated Services Field* (ToS:6):
    - *Premium Services* (PS);
    - *Assured Services* (AS);
    - *Best-Effort* (BE);

Proposta – QoS na Máquina de Criptografia

Fluxo de Dados para Criptografia



- Escalonamento:
  - *Weighted Round Robin* (WRR):
    - Atende as filas em ciclos;
    - Cada fila pode ter um peso diferente para o tempo de atendimento.

Referências

- Barbieri, R., Bruschi, D. e Rosti, E. (2002) “Voice over IPsec: Analysis and Solutions” *Proceedings of the 18th Annual Computer Security Applications Conference*.
- Baugher, M., Mcgrew, D., Naslund, M., Carrara, E. e Norrman, K (2004) “The Secure Real-time Transport Protocol (SRTP)”, IETF RFC 3711, Março.
- Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z. e Weiss, W. (1998) "An Architecture for Differentiated Services", IETF RFC 2475, Dezembro.
- Cisco (2000). Disponível em: http://www.cisco.com/networkers/nw00/pres/2403.pdf;
- Handley, M., Crowcroft, J., Bormann, C., Ott, J. (2000) “The internet multimedia conferencing architecture”. IETF Internet Draft, Julho.
- Hong, K., Jung, S., Iacono, L. L. e Ruland, C. (2004) “Impacts of Security Protocols on Real-Time Multimedia Communications”, *Lecture Notes In Computer Science*, vol. 3325/2005.
- Housley, R. (2004) "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", IETF RFC 3686, Janeiro.
- Kent, S. e Atkinson, R. (1998) “Security Architecture for the Internet Protocol”, IETF RFC 2401, Novembro.
- Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L. E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., Zheng, H. (2001), "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", IETF RFC 3095, Julho.
- Kuhn, D. R., Walsh, T. J., Fries, S. (2005) “Security Considerations for Voice Over IP Systems”, NIST - National Institute of Standards and Technology, Janeiro.
- Schulzrinne, H., Casner, S., Frederick, R. e Jacobson, V. (2003) "RTP: A Transport Protocol for Real-Time Applications”, IETF RFC 3550, Julho.
- Tanenbaum, A. S. (2003) “Redes de computadores“, ed. Rio de Janeiro: Elsevier.
- VoIPSA (2005) “VoIP Security and Privacy Threat Taxonomy”, Outubro.
- Katevenis, M., Sidiropoulos, S. e Courcoubetis, C. (1991) "Weighted round-robin cell multiplexing in a general-purpose ATM switch chip," *IEEE Journal on Selected Areas in Communications*, vol. 9, pp. 1265-79, Outubro.

Investigação e Avaliação do Impacto da Aplicação de Mecanismos de Segurança em *Voice over Internet Protocol* (VoIP)

Rafael Mendes Pereira
Liane M. R. Tarouco