Avaliação de Alternativas para a Diminuição do Impacto da Utilização do IP *Security* em VoIP

Rafael M. Pereira e Liane M. R. Tarouco
rmpereira@inf.ufrgs.br, liane@penta.ufrgs.br

Instituto de Informática – Universidade Federal
do Rio Grande do Sul (UFRGS)

Roteiro

- Introdução
- Riscos
- Soluções
- Impacto
- Alternativas
- Considerações Finais

Introdução

- Voz sobre IP (VoIP):
  - Novos recursos (compartilhamento de dados);
  - Maior flexibilidade e menor custo em relação à comunicação convencional;
  - **Novos riscos!**

Riscos

- 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

- VoIPSA – *VoIP Security Alliance*
- 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 e perdas;
- Fatores:
  - Expansão dos dados;
  - Aumento do Processamento.
  - Perda de Pacotes;
  - Propagação de Erro.

Objetivo

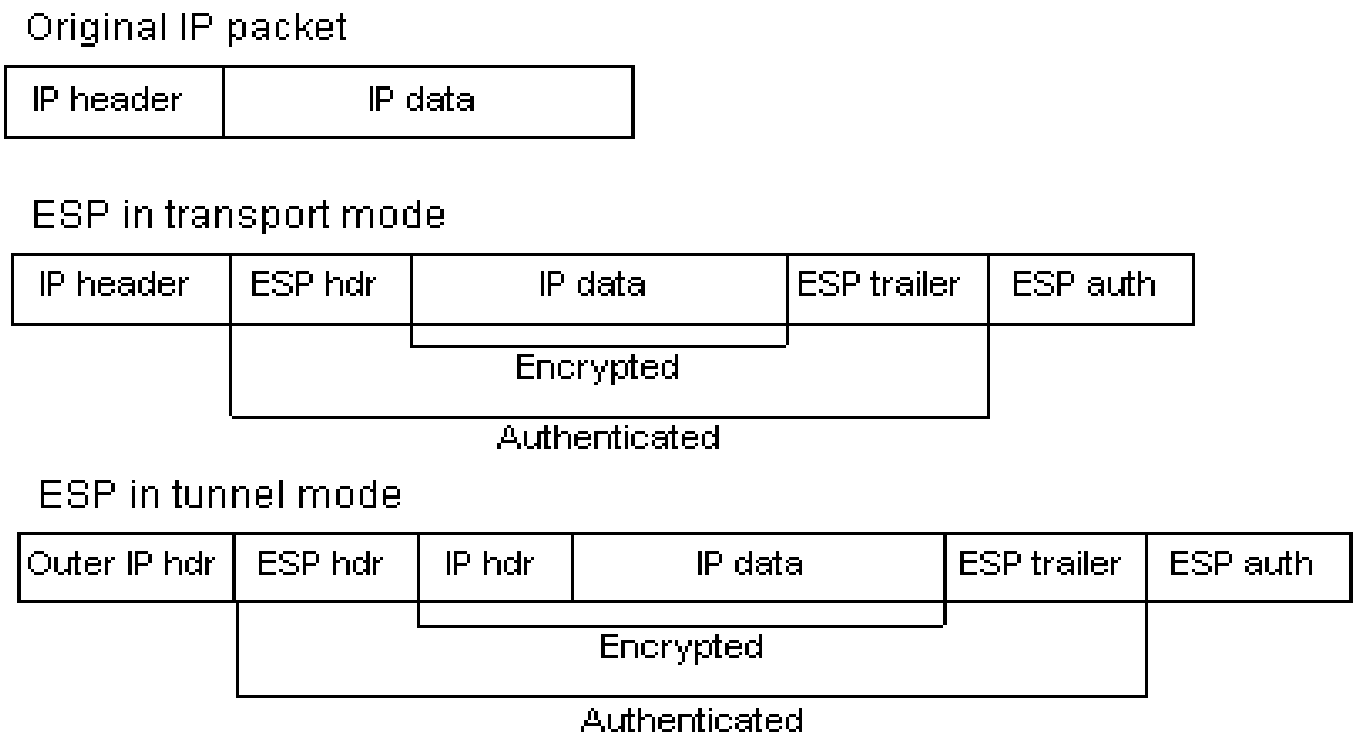
- Identificar e avaliar o impacto da aplicação do IPSec em VoIP;
- Avaliar alternativas para a minimização desse impacto.

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:
  - 3DES (*Triple Data Encryption Standard*);
  - HMAC (*Hashed Message Authentication Code*)
    - MD5 (*Message-Digest algorithm 5*) e SHA-1(*Secure Hash Algorithm*).

Expansão dos Dados

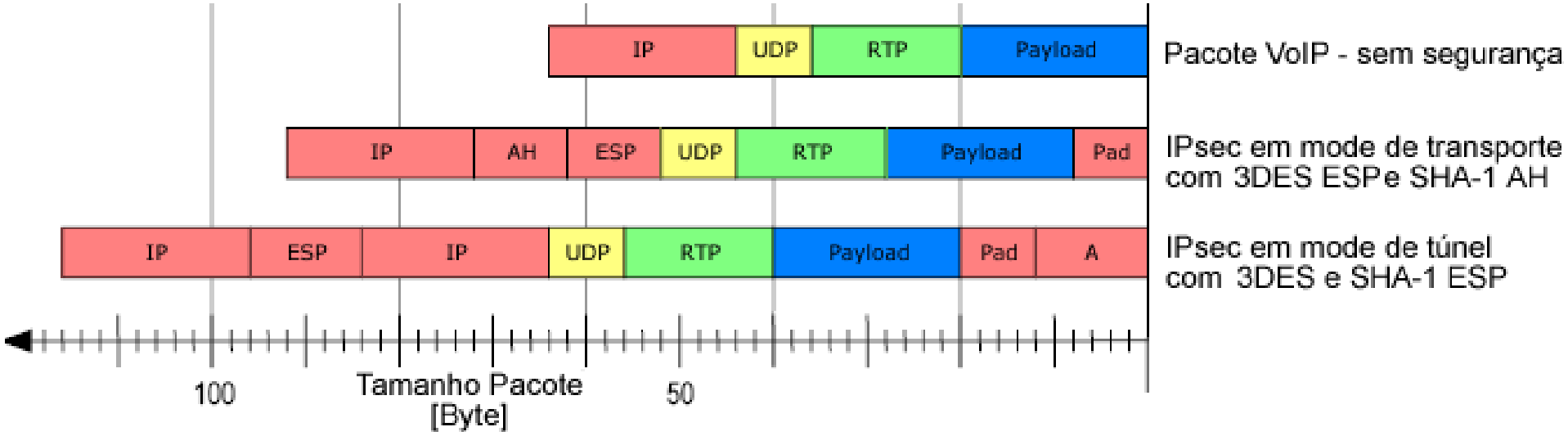
- Cabeçalho ESP:



- *Padding*;

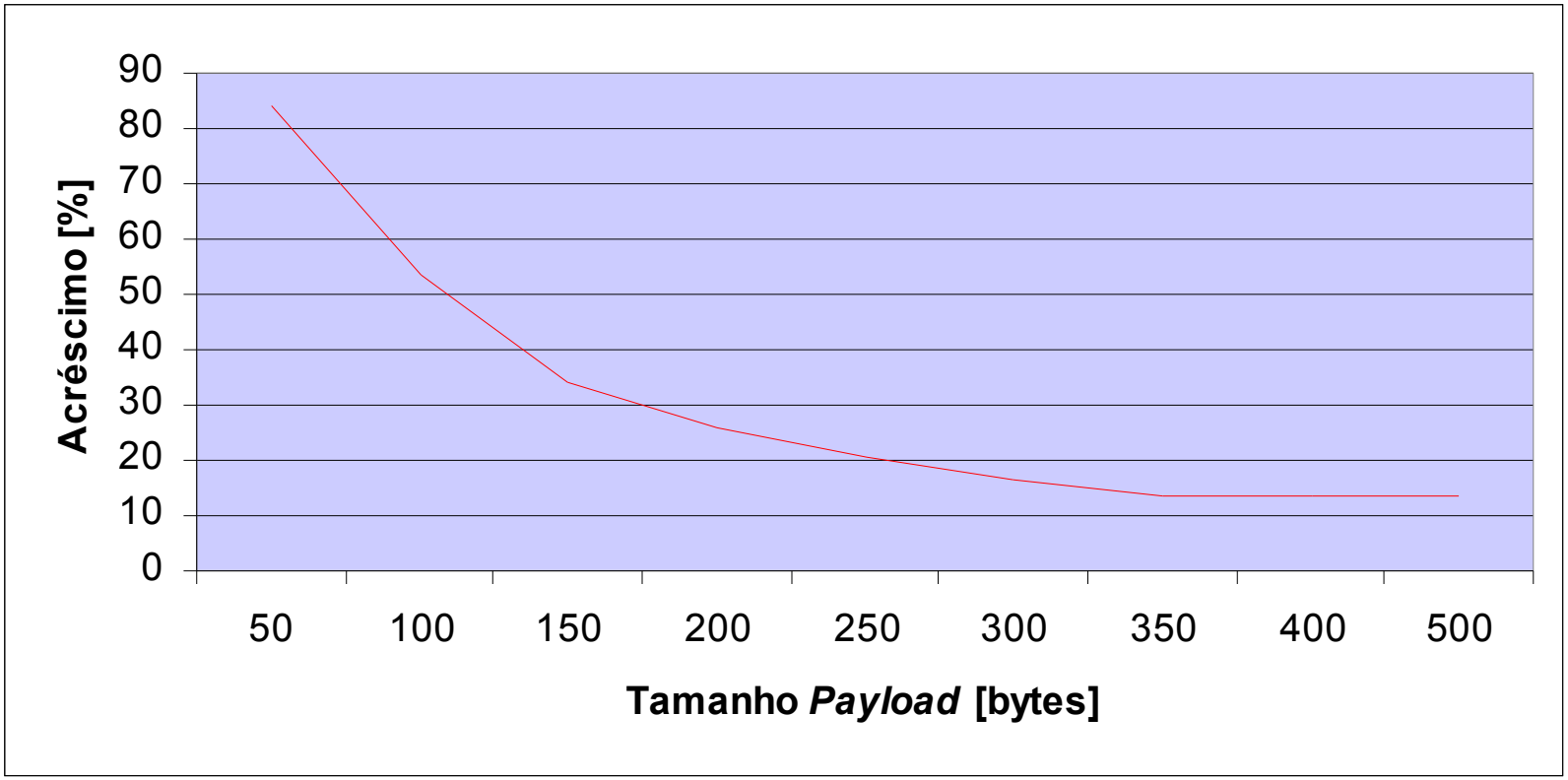
Expansão dos Dados

- Exemplo (*payload* 20 bytes):



Expansão dos Dados

- Acréscimo (%) do Tamanho do Pacote (ESP Modo de Túnel)



Compressão

- cRTP (compress RTP):
  - Não suporta ESP/IP;
- IPHC (IP *Header Compression*):
  - Cabeçalhos: ESP/IP, UDP/IP e TCP/IP;
  - Compressão para até 2 bytes;
  - Menor complexidade de implementação;
  - Ressincronização lenta.
- ROHC (*Robust Header Compression*):
  - Cabeçalhos: ESP/IP, RTP/UDP/IP, UDP/IP e TCP/IP;
  - Compressão para até 1byte;
  - Maior complexidade de implementação;
  - Ressincronização rápida.

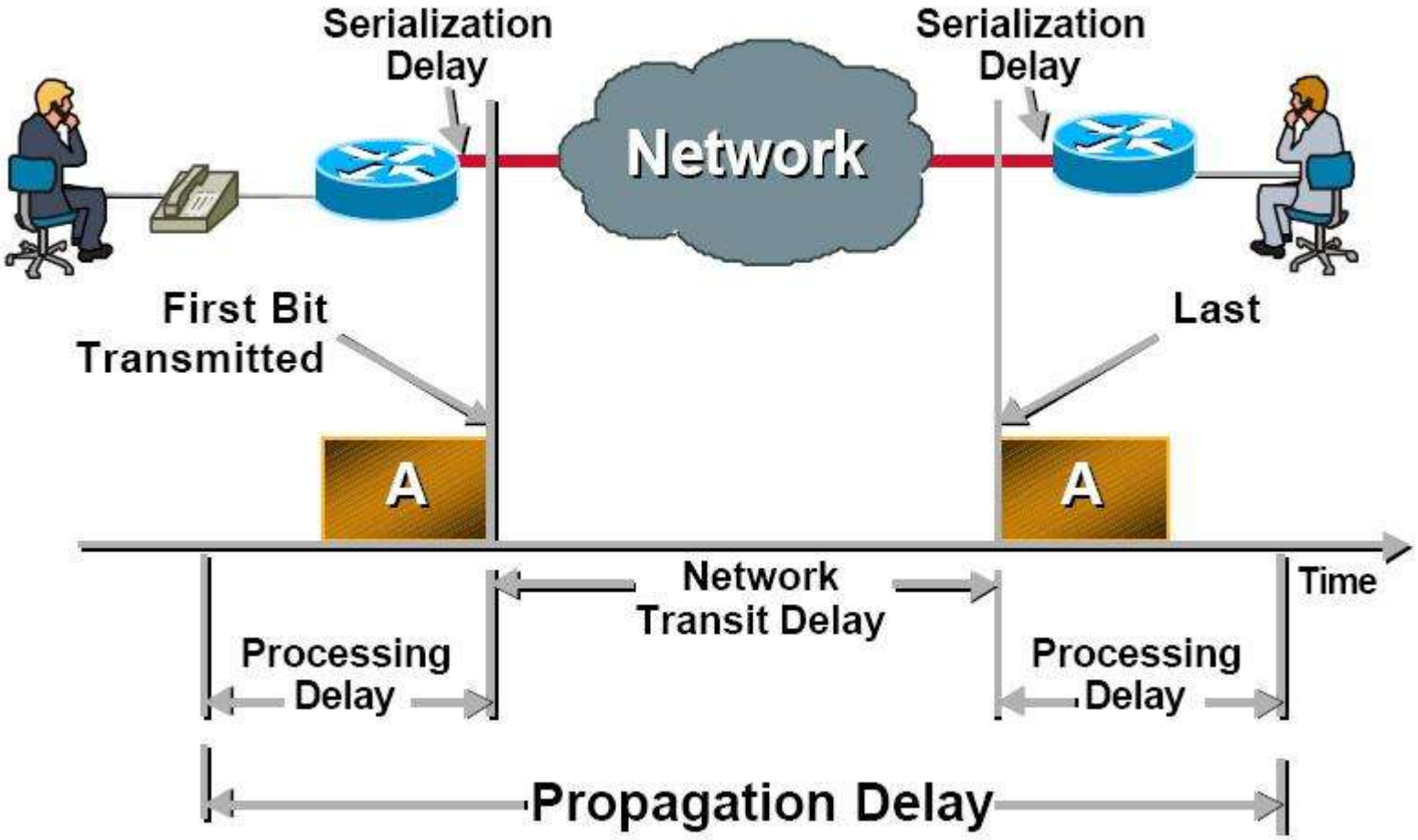
Uso da Banda

- Número máximo de ligações:
  - *Payload* (60 Bytes);
  - *Compress* ESP/IP *Header* (para 4 bytes).

	G.711(64Kbps)		G.729 (8Kbps)		G.723.1(6.3Kbps)	
Link	ESP/IP	Compress	ESP/IP	Compress	ESP/IP	Compress
150kb/s	3	5	3	5	5	7
500kb/s	11	16	11	16	16	23
1Mb/s	22	31	22	31	32	46
5Mb/s	110	156	110	156	161	230

  - Ganho 45%

Atraso


Serialization Delay
Serialization Delay
Network
First Bit Transmitted
Last
A
A
Network Transit Delay
Time
Processing Delay
Processing Delay
Propagation Delay

Atraso - VoIP

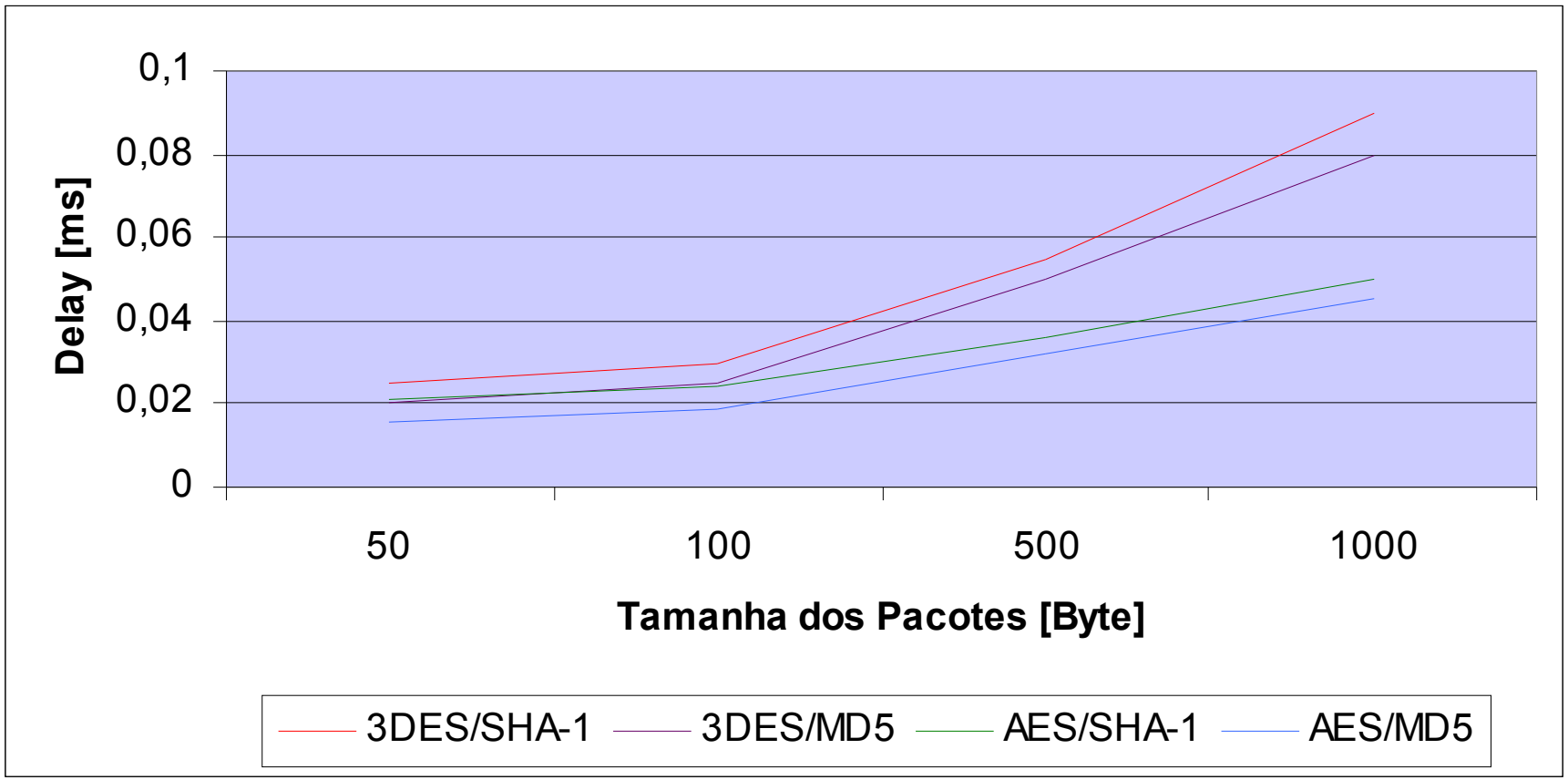
- Atraso fim-a-fim:
  - 0ms - 150ms (Bom);
  - 150ms - 300ms (Aceitável);
  - Maior que 300ms (Inaceitável).
- Atraso codificação: 1ms a 30ms;
- Atraso transmissão (*link delay*, *jitter buffer*, etc): 100 ms;
- Atraso adicional:
  - 0ms - 20ms (Bom);
  - 20ms - 50ms (Aceitável);
  - Maior que 50ms (Inaceitável).

Atraso - IPSec

- Encriptação (IP header||UDP header||RTP header||RTP Payload);
- ESP header;
- MAC (ESP header||UDP header||RTP header|| RTP Payload);
- Novo IP header.

Atraso - IPSec

AMD Serpron (1.6 GHz, 448 MB de RAM) – Linux 2.6 (NETKEY – openswan)



Perda de Pacotes - VoIP

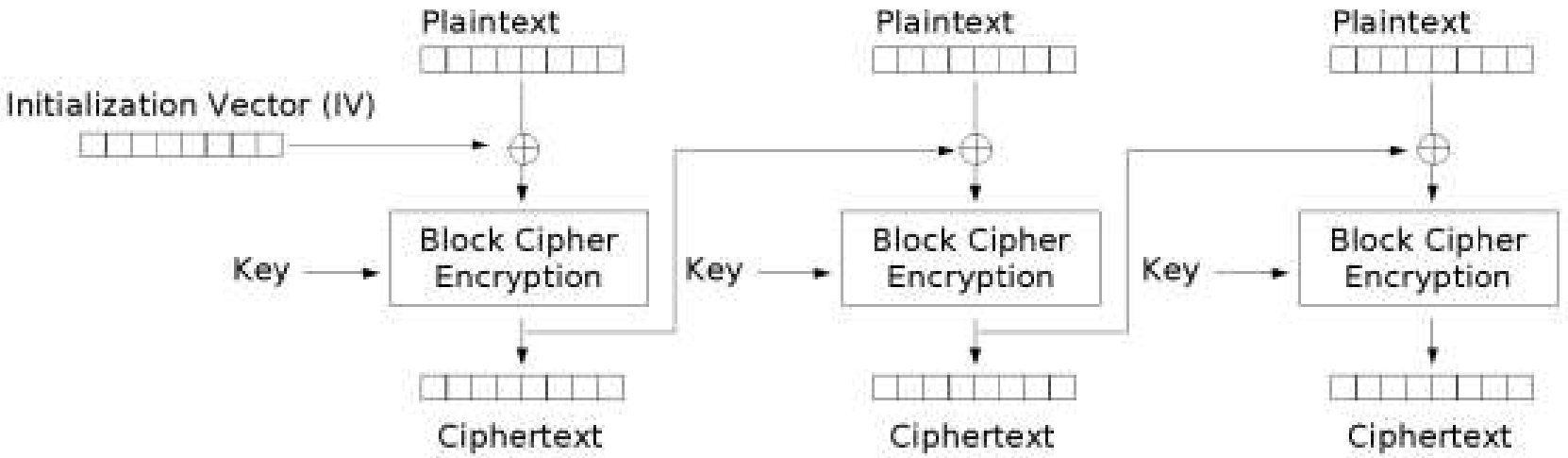
- Perda de pacotes:
  - 0%-0.5% (Bom);
  - 0.5%-1.5% (Aceitável);
  - >1.5% (Inaceitável).

Perda de Pacotes – IPSec

- Integridade;
- Modo de Cifragem em Bloco
  - CBC - *Cipher-block chaining* (Padrão)
  - Tamanho dos Blocos:
    - AES: 16 Bytes;
    - 3DES: 8 Bytes.

Perda de Pacotes - IPSec

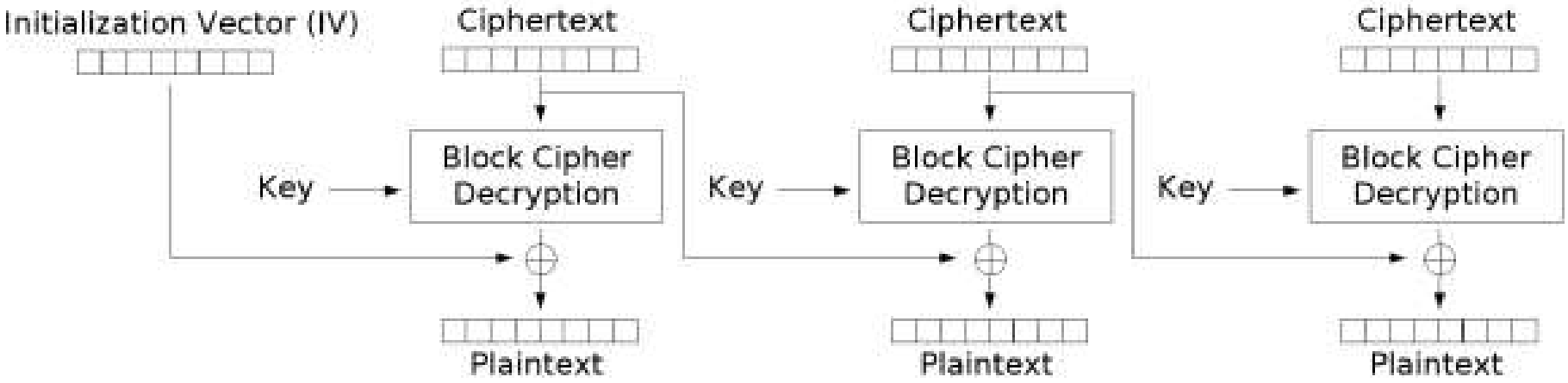
- CBC - Encriptação



Cipher Block Chaining (CBC) mode encryption

Perda de Pacotes - IPSec

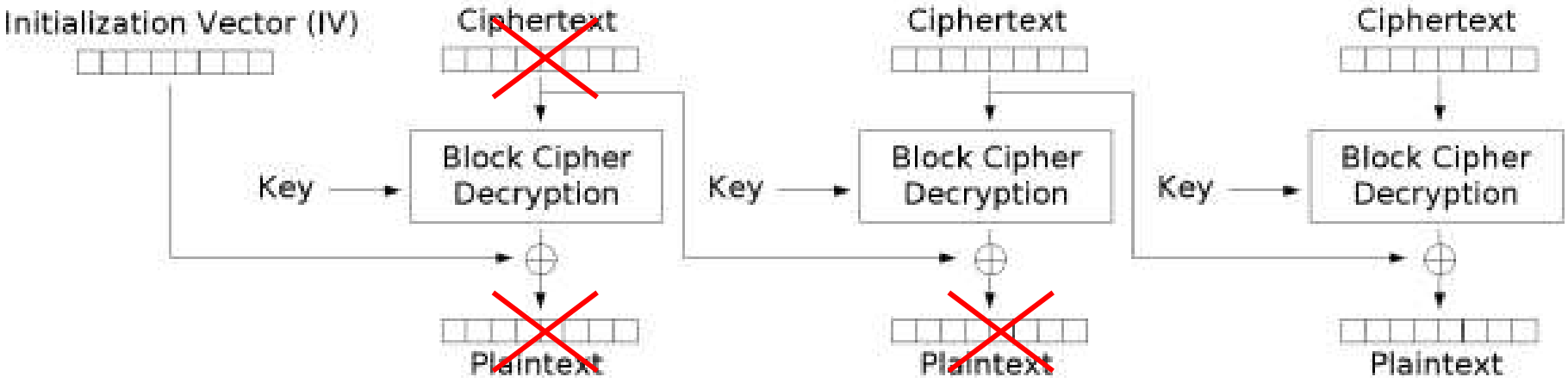
- CBC - Decriptação



Cipher Block Chaining (CBC) mode decryption

Perda de Pacotes - IPSec

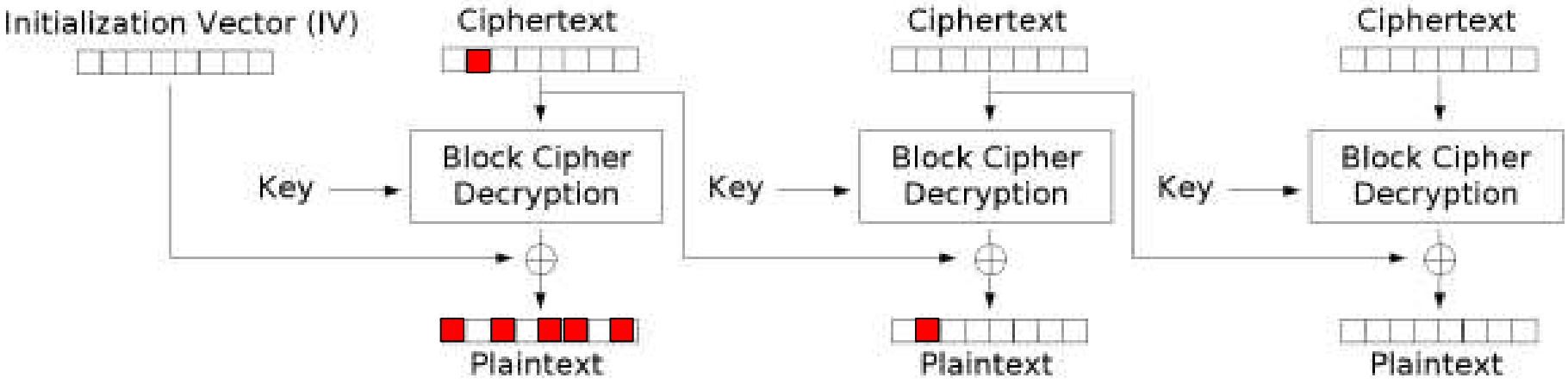
- CBC - *Packat Loss*



Cipher Block Chaining (CBC) mode decryption

Propagação de Erro - IPSec

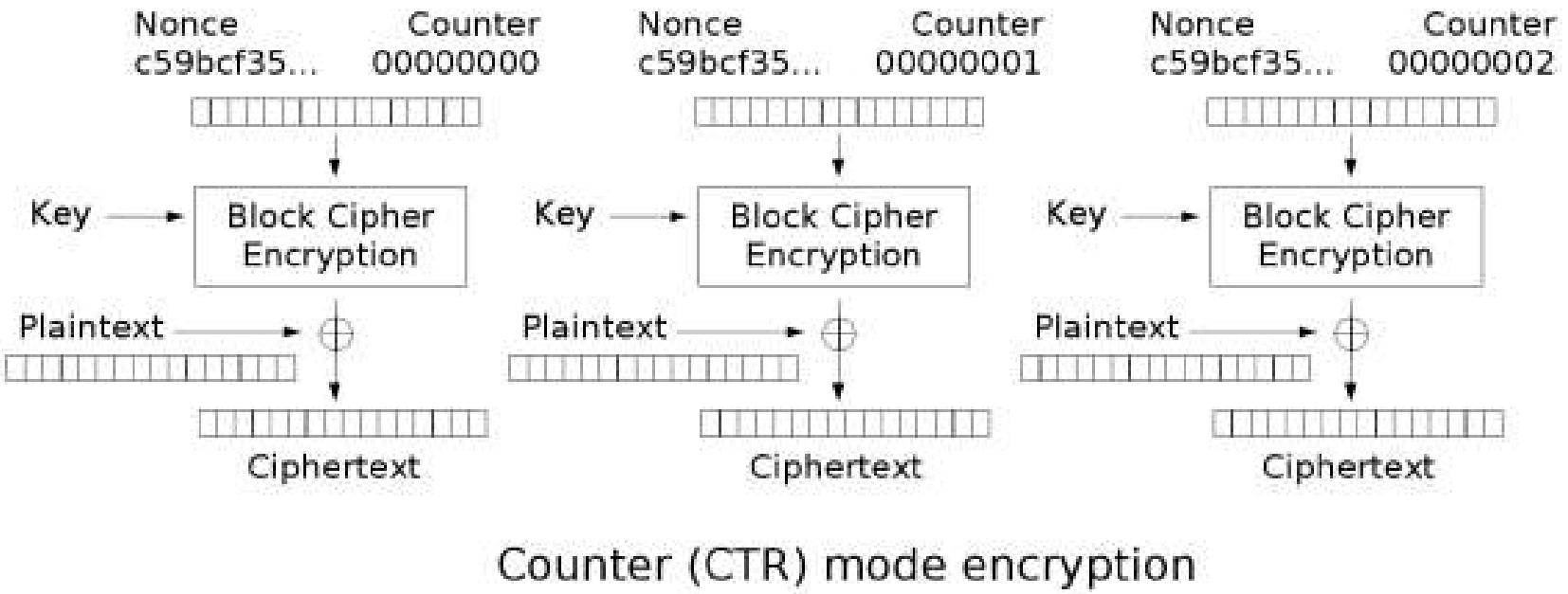
- CBC - bit *error*



Cipher Block Chaining (CBC) mode decryption

Perda de Pacotes - IPSec

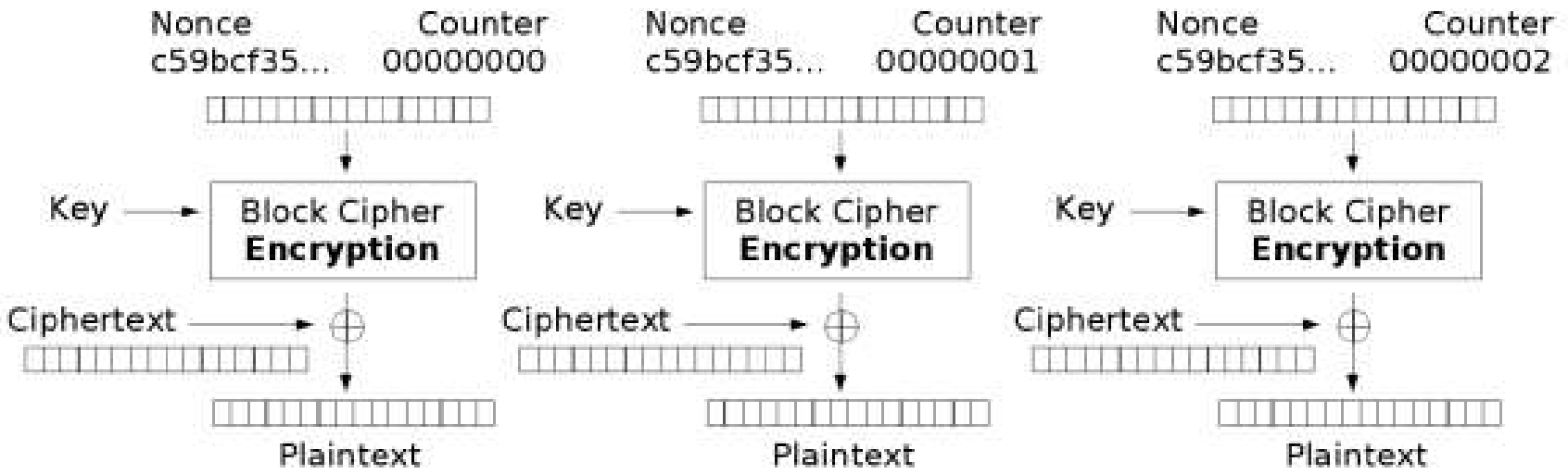
- CTR – *Counter mode* (Alternativa)



Counter (CTR) mode encryption

Perda de Pacotes - IPSec

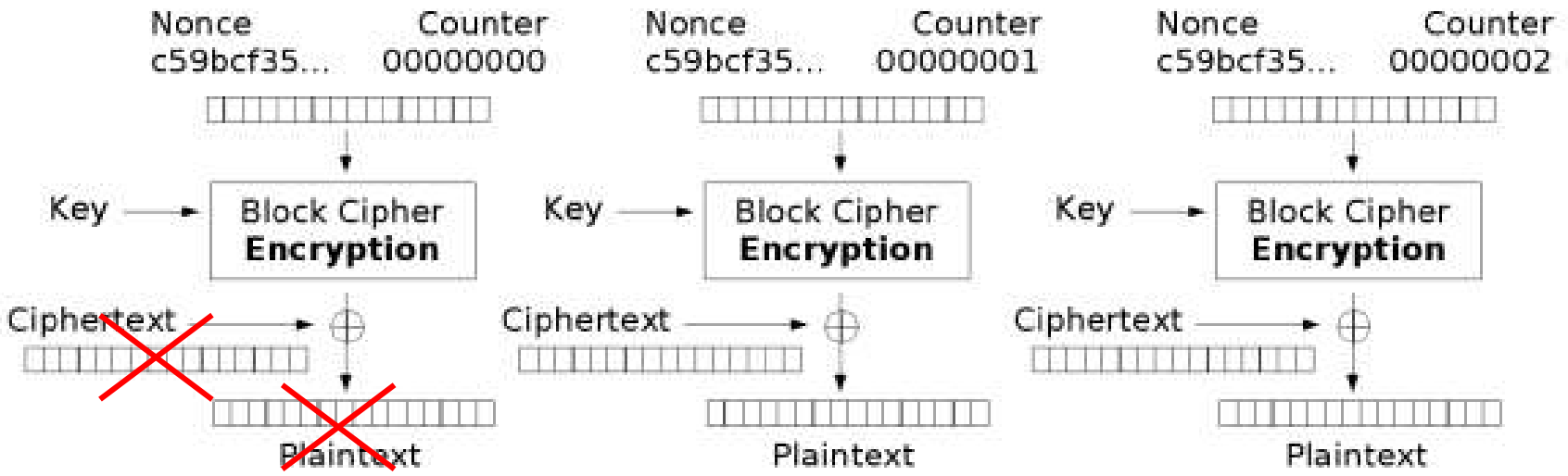
- CTR - Decriptação



Counter (CTR) mode decryption

Perda de Pacotes - IPSec

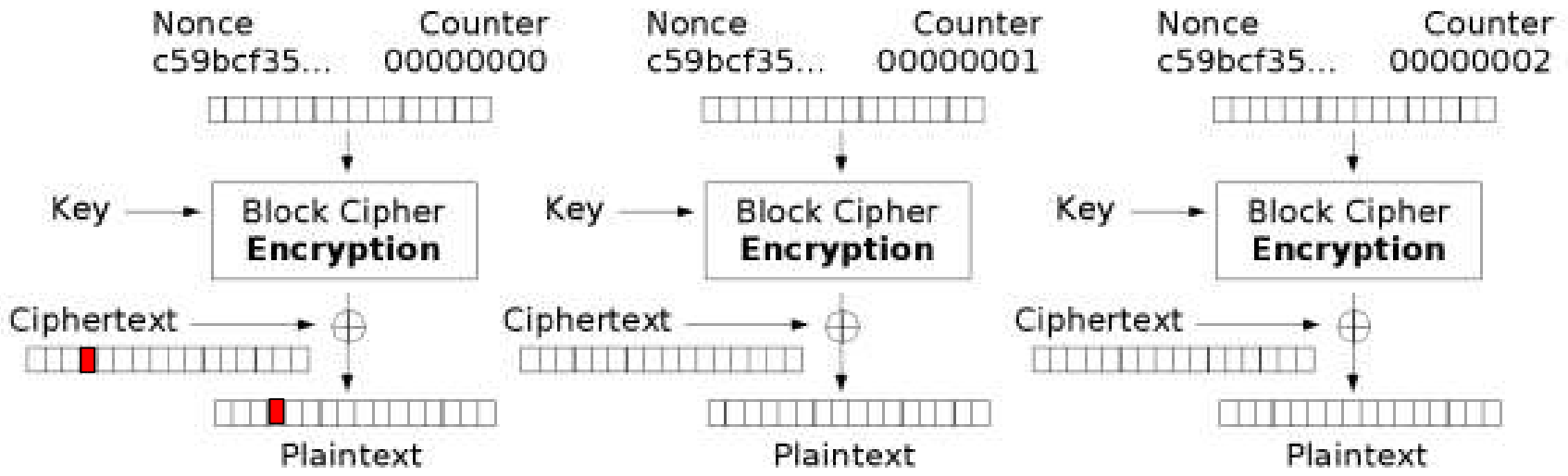
- CTR - *Packat Loss*



Counter (CTR) mode decryption

Propagação de Erro - IPSec

- CTR - bit *error*



Counter (CTR) mode decryption

Overhead?

- Em desenvolvimento:
- Compressão:
  - Extensão da Free ROHC (rohc.sourceforge.net): suporte ESP/IP;
- Modo de cifragem:
  - Extensão da Openswan (www.openswan.net): suporte CTR;

Considerações Finais

- Necessária a aplicação de métodos de compressão em conjunto ao IPSec em VoIP.
- Criptografia e Autenticação no IPSec não afetam substancialmente no atraso fim-a-fim em VoIP;
- CTR apresenta como uma boa alternativa ao modo CBC.

Obrigado.
Perguntas?

Rafael M. Pereira, Liane M. R. Tarouco
rmpereira@inf.ufrgs.br, liane@penta.ufrgs.br