# IP Security ソフトウェア処理の性能評価

慶應義塾大学 環境情報学部
有賀 征爾

## IPSec

- 認証と暗号化
  - AH　Authentication Header
    - 認証
  - ESP　Encapsulating Security Payload
    - 暗号化
- 利点
  - 安全な通信の透過的な実現
- 欠点
  - 通信性能の低下

# 本研究の目的

- 大容量なトラヒックを生成するアプリケーションとIP Securityを同時に用いた場合の性能測定
  - 実験室環境での基礎データの収集と分析
  - 実トラヒック環境における実践的なデータの収集と解析

**次世代インターネット環境のアプリケーションを想定**



# 実験に関する共通の条件

- Transport モードで計測
- 鍵の設定はすべて手動

# 実験

- 実験室環境
  - 同一リンク上での計測
  - ルータを介しての計測
- 広域ネットワーク
  - Digital Video を用いた実トラヒック環境での計測

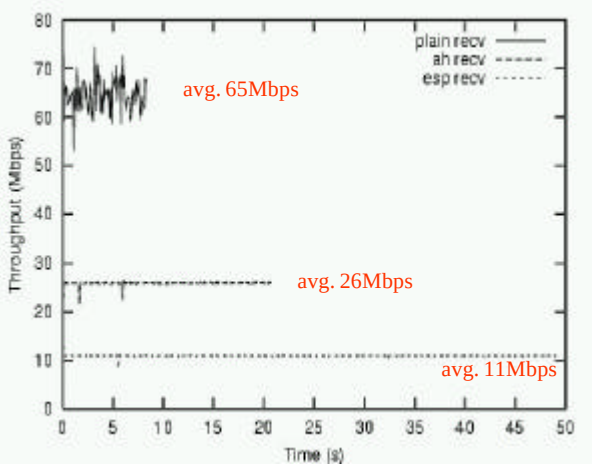


# 実験（その1）
## 同一リンク上の2ホスト間の場合

- 環境
  - 2台の計算機をクロスケーブルで接続
  - PentiumII450MHz
  - Intel EtherExpress Pro 100
  - 暗号アルゴリズム
    - AH: HMAC-SHA1
    - ESP: 3DES-CBC
- 内容
  - TCPの転送速度を計測 (DBS)
  - システムの資源割り当てを変化させて計測
  - アプリケーションからアプリケーションまでの計測

# 資源をできるだけ割当てた場合

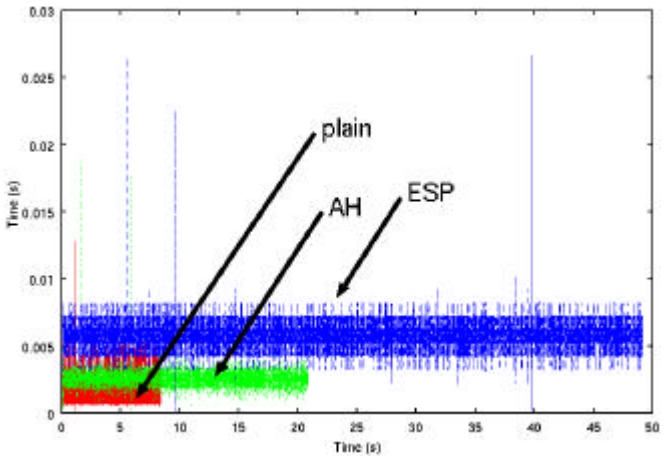
## Throughput





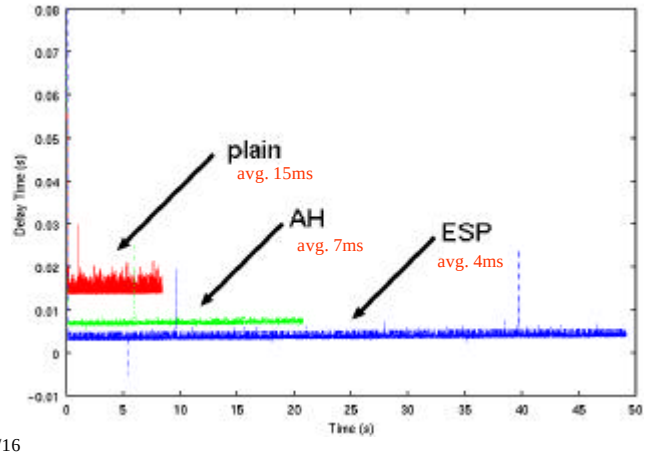

# 資源をできるだけ割当てた場合(2)

## Jitter



# 資源をできるだけ割当てた場合(3)

## Delay

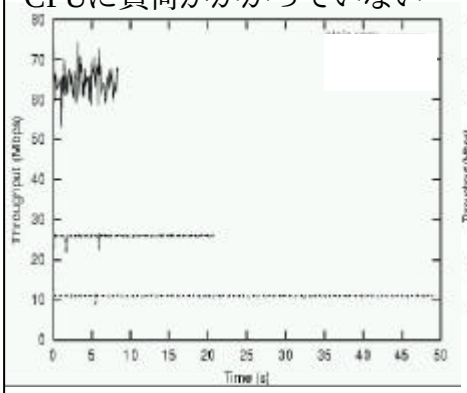




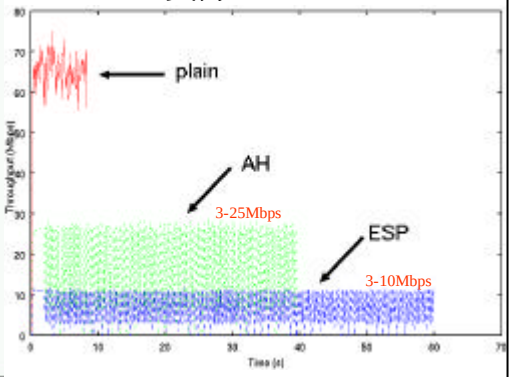

# システムの資源が
# 他にも割当てられている場合

## Throughput

CPUに負荷がかかっていない




CPUに負荷がかかっている



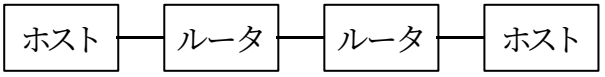
# 実験

- 実験室環境
  - 同一リンク上での計測
  - ルータを介しての計測
- 広域ネットワーク
  - Digital Video を用いた実トラヒック環境での計測



# 実験（その2）
## ルータを経由する場合

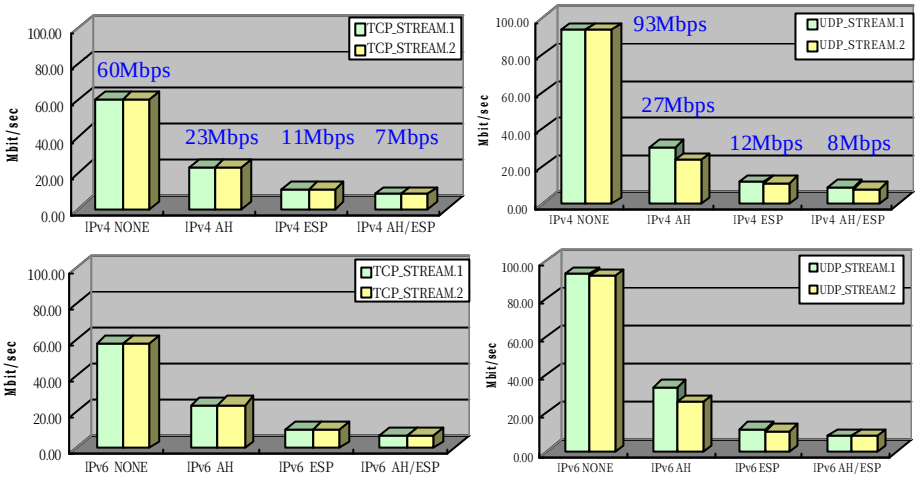
- 環境
  - ホスト:Pentium450MHz
  - ルータ:Pentium500MHz
  - Intel EtherExpress Pro 100




FastEthernet

- 内容
  - TCP, UDPの転送速度を計測 (netperf)
    - STREAM, REQUEST/RESPONSE
  - IPv4, IPv6
  - AH, ESP, AH/ESP
    - AH: HMAC-SHA1 / ESP: 3DES-CBC

# STREAMテスト

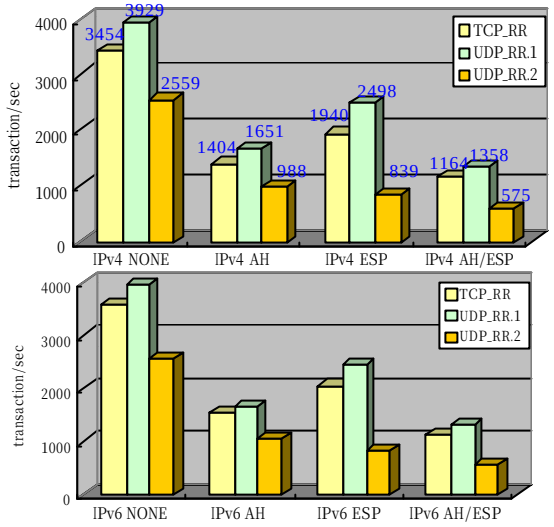





# STREAMテスト(2)

- IPSecを使用した場合 throughput が低下
- TCPとUDPの比較
  - AH, ESPの処理がボトルネック
  - メッセージサイズに反比例せず
- AHとESPの比較
  - AHはESPの約2倍のスループット
- IPv4とIPv6
  - ほぼ差はない

# REQUEST/RESPONSEテスト






# REQUEST/RESPONSEテスト(2)

- IPSecを使用した場合の性能低下
- TCPとUDPの比較
  - メッセージサイズが小さいときは、IPSecはボトルネックにはなっていない
- AHとESPの比較
  - メッセージサイズが小さい場合，ESPのパフォーマンスの方が上
- IPv4とIPv6の比較
  - ほぼ差はない

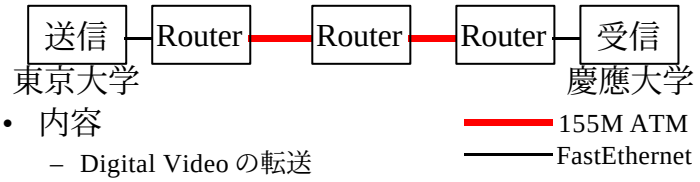
# 実験

- 実験室環境
  - 同一リンク上での計測
  - ルータを介しての計測
- 広域ネットワーク
  - Digital Video を用いた実トラヒック環境での計測



# 実験（その3）
## 実トラヒック環境の場合

- 環境
  - 送信: PentiumII 400MHz
  - 受信: PentiumII 450MHz
  - AH: HMAC-SHA1 / KEYED-SHA1
  - ESP: 3DES-CBC / Blowfish-CBC



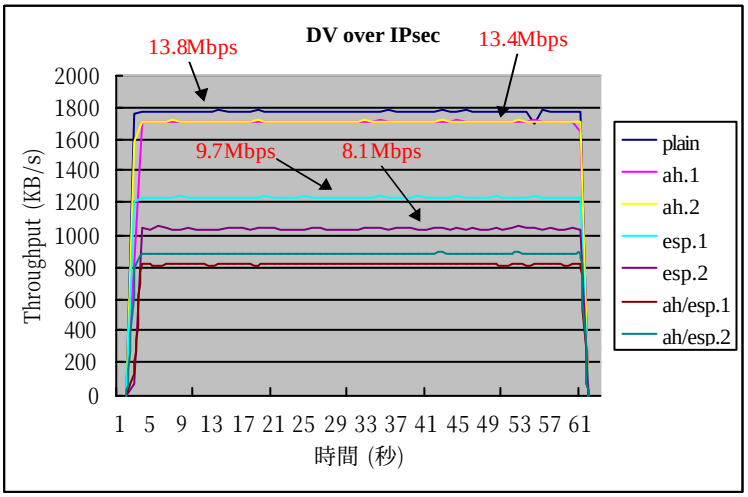

- 内容
  - Digital Video の転送
  - 受信ホストの netstat で計測
  - IPv6での計測

# Digital Video

- UDP
- Payload size は 約500byte
- Frame rate は フルレート で実験
  - 通常 30Mbps くらい



# Digital Video の転送



# Digital Video の転送(2)

- 実験室環境と実ネットワークの比較
  - AHを使用したときは，ネットワークがボトルネック
  - ESPを使用したときは，ESPがボトルネック
- アルゴリズムによる差
  - 3DESとBlowfishのスループットに20%程度の差



# まとめ

- 性能評価
  - IPSecを使用したパケット転送性能を実データとして収集
    - 実験室環境での基礎データ
      - ネットワークトポロジによる差
      - AHとESPの性能差
      - アルゴリズムによるパフォーマンスの差
- 実環境への適用
  - 実験室環境との比較
    - 高精細動画像（DV)による実験
      - 他の要因によって左右
      - 実ネットワークでは必ずしもIPSecがボトルネックとはならない