VLIV ZABEZPEČENÍ SÍŤOVÉ INFRASTRUKTURY NA KVALITU HOVORU

Jiří Škrobák

19.listopadu 2009

OBSAH

- Úvod
- TLS
- OpenVPN
- Jak probíhalo měření
- Kalkulace
- Dosažené výsledky

ÚVOD

- Dvě možnosti zabezpečení – VoIPSec, TLS
- Zpráva se zabývá pouze výzkumem TLS
- Testy v minulosti ukázaly zřejmý dopad zabezpečení na kvalitu hovorů avšak výsledky byly zveřejněny bez přesných kalkulací
- Testované metody jsou platné pro TLS a byly testovány na OpenVPN

TLS

- Kryptografický protokol
- Tři fáze:
  - dohoda na algoritmech
  - výměna klíčů a autentizace
  - symetrické šifrování dat
- K datové výměně použito symetrické šifrování kvůli rychlejšímu zpracování
- Koncové body – server, client

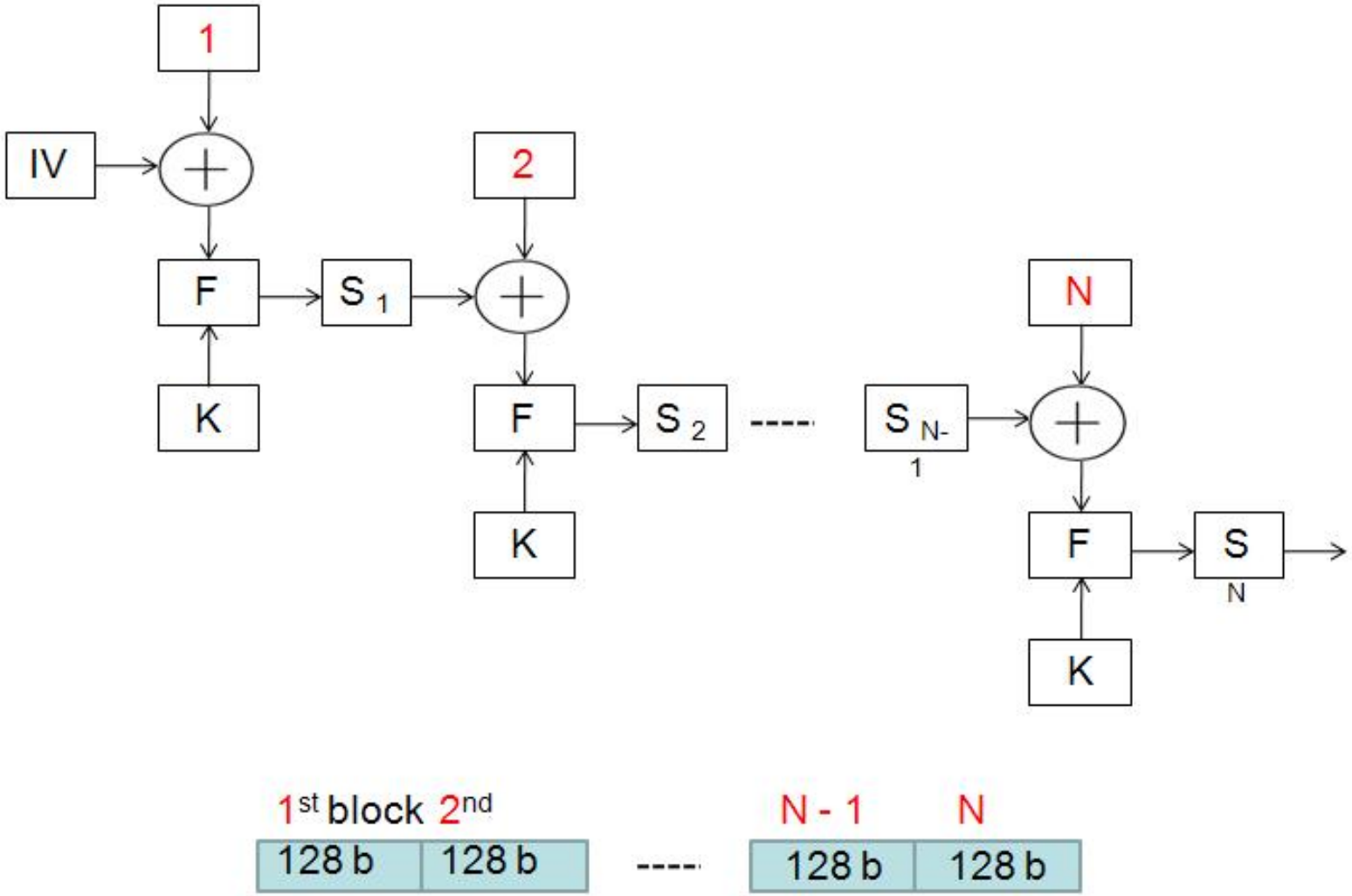
OPENVPN

- Technologie na konstrukci privátních sítí
- Jeden z nejpopulárnějších produktů
- Flexibilní
- Opensource
- Cenově výhodný
- Široce testovaný
- Uživatelsky nenáročný

OPENVPN (2)

- Není nutno konfigurovat NAT na vytvoření privátní sítě
- Nekompatibilní s IPSec
- Využívá knihovny OpenSSL pro zašifrování dat a kanálů
- V konfiguračních souborech je zadán typ šifrovacího algoritmu (AES, DES, 3DES, Blowfish) – ovlivní počet bloků

CIPHER BLOCK CHAINING



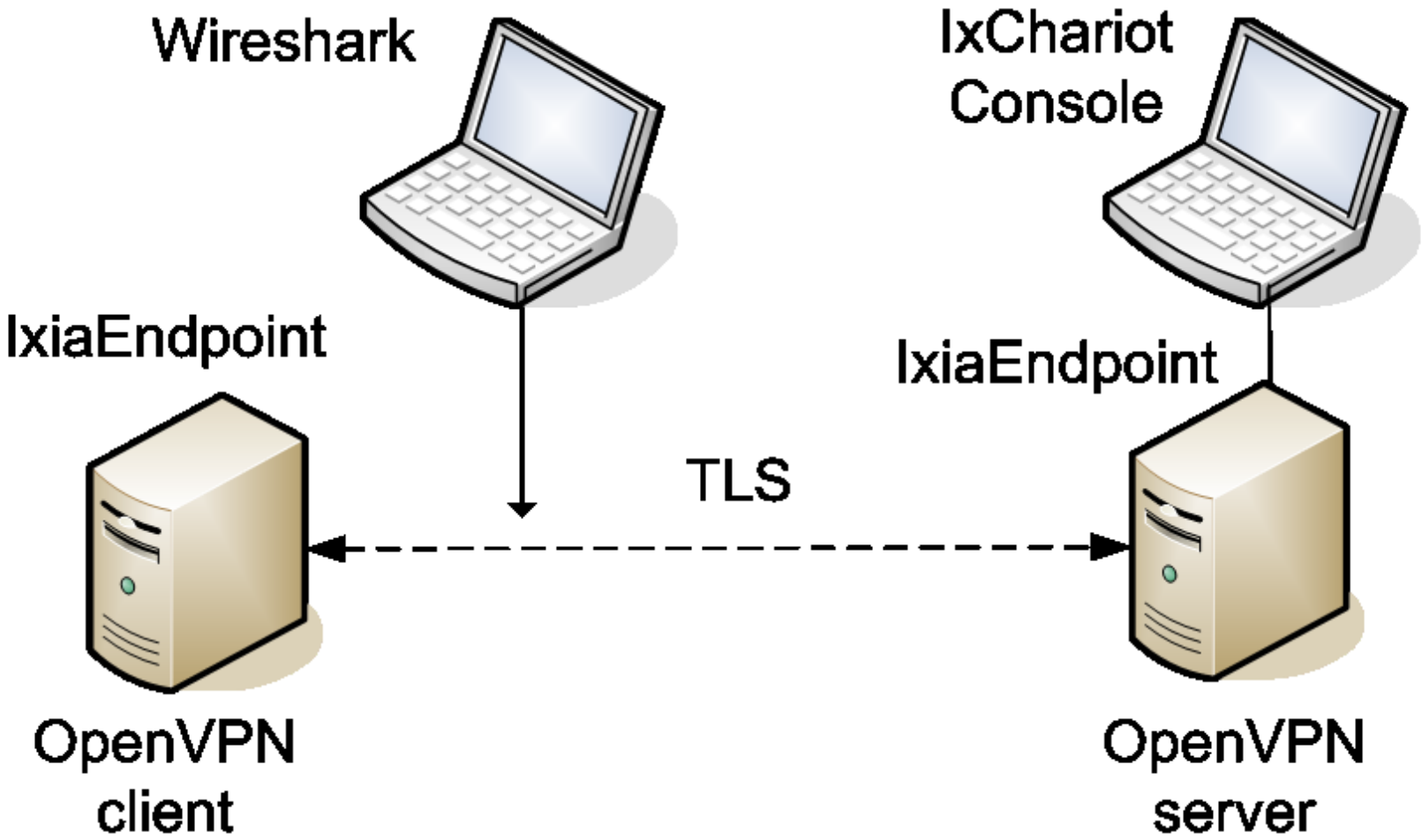
VELIKOSTI KLÍČŮ

- DES-CBC 64 bit default key (fixed)
- RC2-CBC 128 bit default key (variable)
- DES-EDE-CBC 128 bit default key (fixed)
- DES-EDE3-CBC 192 bit default key (fixed)
- DESX-CBC 192 bit default key (fixed)
- BF-CBC 128 bit default key (variable)
- RC2-40-CBC 40 bit default key (variable)
- CAST5-CBC 128 bit default key (variable)
- RC2-64-CBC 64 bit default key (variable)
- AES-128-CBC 128 bit default key (fixed)
- AES-192-CBC 192 bit default key (fixed)
- AES-256-CBC 256 bit default key (fixed)

JAK PROBÍHALO MĚŘENÍ

- Měření prováděno na OpenVPN s použitím softwaru IxChariot
- OpenVPN struktura:
  - Client, Server, Wireshark
- IxChariot struktura:
  - Endpoints, Console

SCHÉMA


Wireshark
IxChariot Console
IxiaEndpoint
IxiaEndpoint
TLS
OpenVPN client
OpenVPN server

POŽADAVKY NA ŠÍRKU PÁSMA

- Vysílací strana provádí základní kroky, které mají vliv na šířku pásma:
  - Šifrování
  - Paketizace
  - Časování

KALKULACE

- Proces časování : (1) $$\Delta t = \frac{P_S}{C_R}$$

- Časování může být také odvozeno z obsahu RTP paketu:

(2) $$\Delta t = \frac{\text{timestamp}_{\{N+1\}} - \text{timestamp}_{\{N\}}}{\text{sampling\_frequency}}$$

KALKULACE (2)

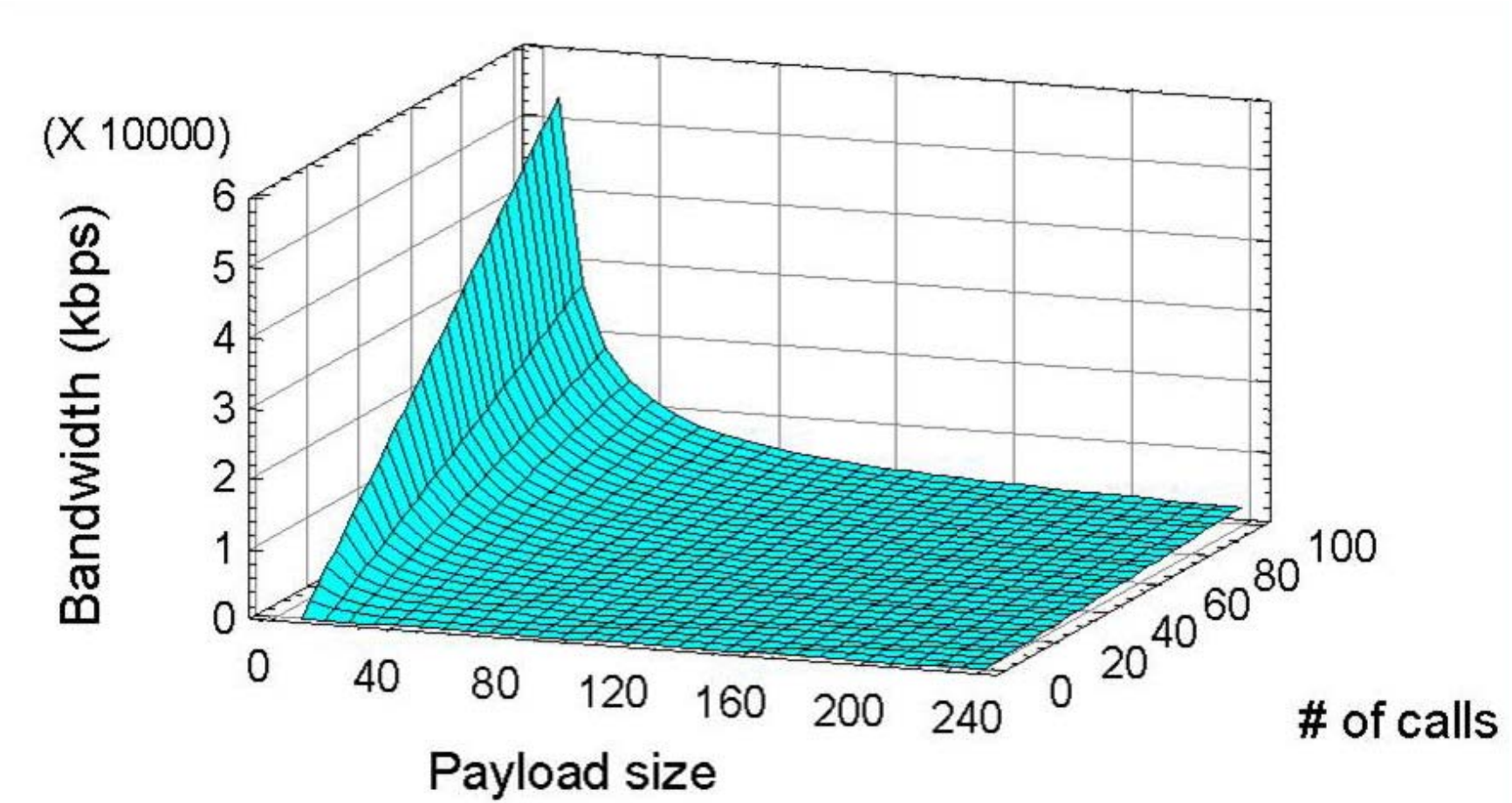
- Velikost paketu na aplikační vrstvě:

$$(3) \qquad S_{AL} = H_{RTP} + P_S$$

- Odvození velikosti $S_F[b]$ rámce na linkové vrstvě:

$$(4) \qquad S_F = S_{AL} + \sum_{j=1}^{3} H_j$$

VZTAH MEZI ŠÍŘKOU PÁSMA, VELIKOSTÍ DATOVÉ ČÁSTI A POČTU SOUBĚŽNÝCH HOVORŮ



KALKULACE (3)

- Požadovaná šířka pásma: (5) $$BW_M = \sum_{i=1}^{M} \frac{S_{Fi}}{\Delta t_i}$$

- Výsledek aplikace vzorce 1,2 a 4 na vzorec 5:

$$BW_M = MC_R \left(1 + \frac{H_{RTP} + \sum_{j=1}^{3} H_j}{P_S}\right)$$

VLIV NA R-FAKTOR

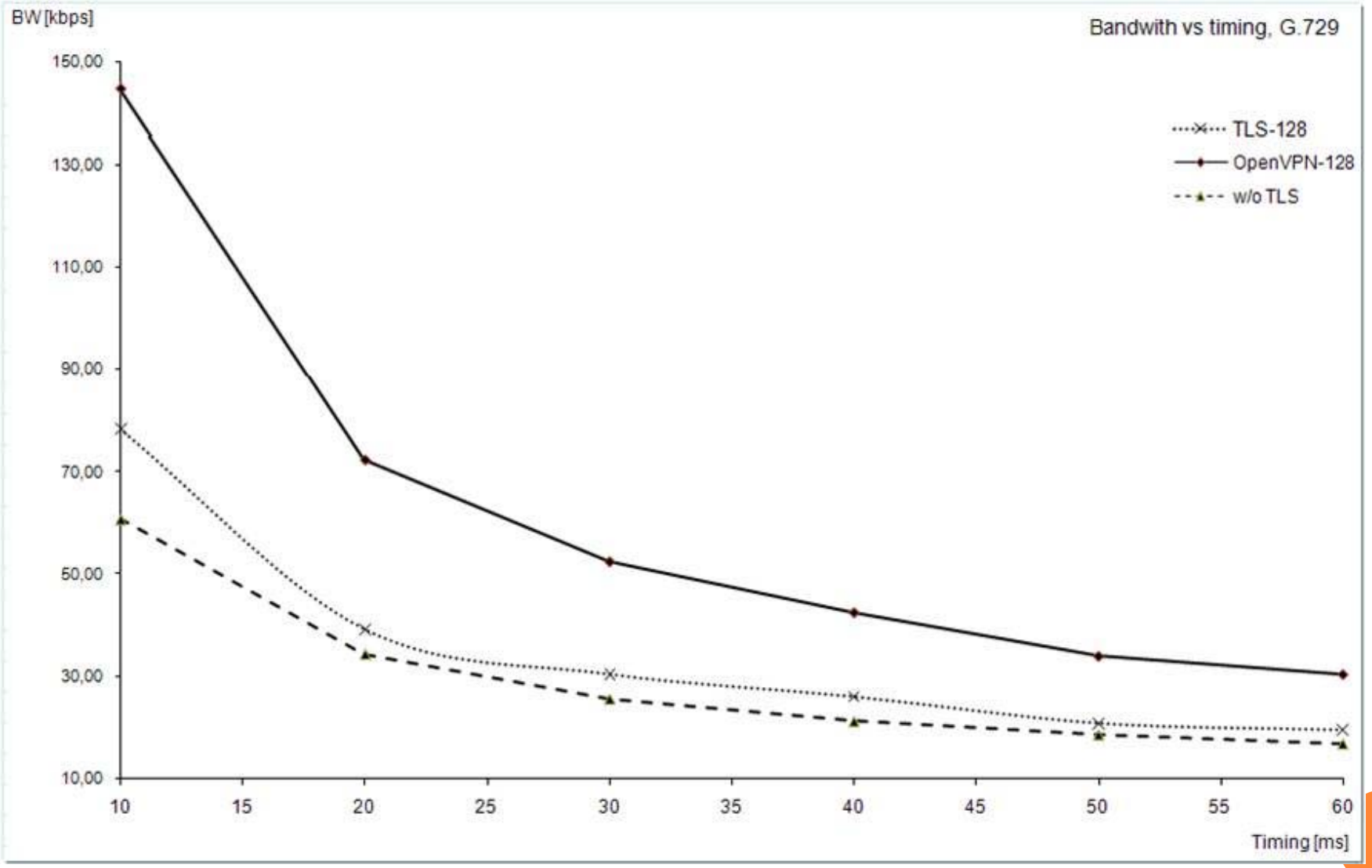
- Celková kvalita je vypočítána vzorcem:

$$R = R_0 - I_S - I_D - I_{E\text{-}EF} + A$$

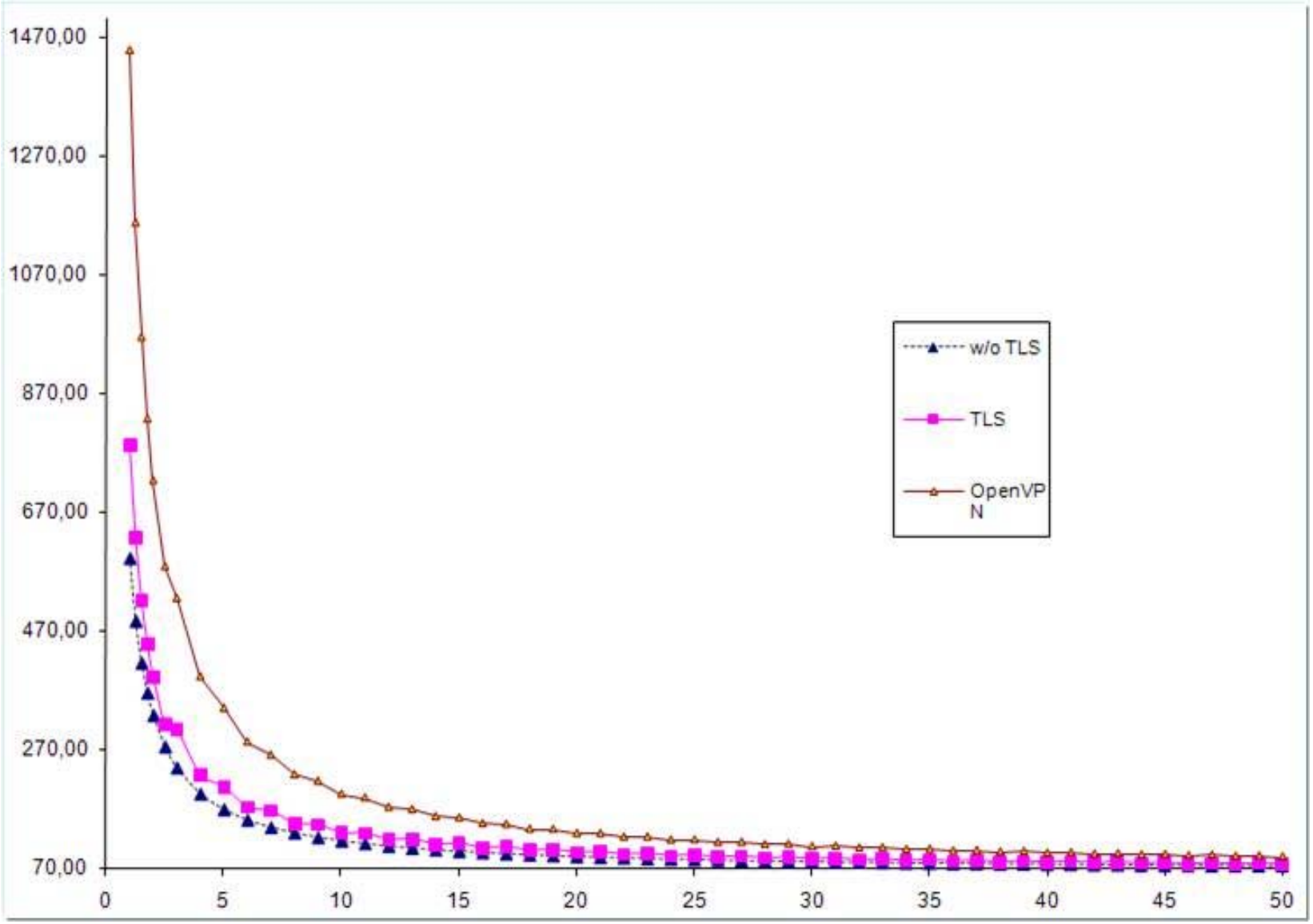
$$I_{E-EF} = I_E + (95 - I_E) \cdot \frac{P_{pl}}{\frac{P_{pl}}{BurstR} + B_{pl}}$$

$$BurstR = \frac{1}{p + q}$$

DOSAŽENÉ VÝSLEDKY



DOSAŽENÉ VÝSLEDKY (2)



ZÁVĚR

- Real time aplikace jsou citlivé na ztrátu paketů
- Použití OpenVPN má své výhody a nevýhody
- Experimenty s konfigurací TLS a OpenVPN naznačily cestu jak nastavit časování a optimalizovat spotřebu kapacit sítě
- Kodeky jsou proti ztrátám různě odolné

DĚKUJI ZA POZORNOST