Kvantově zabezpečený přenos na 100 Gb/s v reálné síti

18.12.2025 - | CESNET

CESNET úspěšně otestoval kombinaci QKD a postkvantové kryptografie na provozní trase v Praze.

Pracovníci sdružení CESNET ověřili v rámci projektu NESPOQ, že kvantová distribuce klíčů (QKD) a postkvantová kryptografie (PQC) mohou spolehlivě chránit datové přenosy na 100Gb/s provozní lince v reálném síťovém prostředí. Na provozní trase dlouhé 9,1 km mezi laboratoří CESNET TLH a pražskou DC Tower prokázali, že kombinace QKD systému IDQ Clavis3 a šifrovacích jednotek vyvinutých na Vysokém učení technickém v Brně (VUT) dokáže zajistit bezpečný přenos i u náročných multimediálních a velkoobjemových dat.

Hlavním cílem testování bylo demonstrovat společné využití QKD systému IDQ Clavis3 jako klíčové bezpečnostní komponenty pro ochranu datových linek s rychlostí až 100 Gb/s v sestavě s šifrovacími jednotkami, které byly navrženy a vyvinuty spoluřešitelem projektu – Vysokým učením technickým v Brně.

QKD a postkvantová kryptografie v reálném metropolitním prostředí
Celková délka optické trasy v městském prostředí činila 9,1 km. Vzhledem k tomu, že kvantový kanál vyžaduje obvykle vyhrazené vlákno, bylo nezbytné sloučit existující datový provoz a servisní kanály QKD systému ve spektrální oblasti pomocí filtrační soustavy do druhého vlákna. Použitím filtrační soustavy narostl významně celkový útlum v optické trase, a to tak, že do přijímače dorazí pouhé 1 % optického výkonu vysílače. Proto bylo zapotřebí pro realizaci přenosu zabezpečeného šifrovaného kanálu použít vysokorychlostní DWDM přenosový systém Ribbon.

Ověření funkčnosti na běžných i multimediálních datech
V reálném prostředí proběhla série testů ověřujících funkčnost zabezpečeného kanálu při přenosu citlivých dat. Kromě verifikačního uměle generovaného provozu byly testovány i běžné typy datových přenosů, například přenos souborů nebo 4K video stream zprostředkovaný technologií Modular Video Transmission Platform (MVTP). Při přenosu komprimovaného 4K video streamu zabezpečeným kanálem se pohyboval datový tok okolo 220 Mb/s. Celý přenos proběhl zcela bezchybně přes šifrovaný kanál, čímž byla ověřena stabilita řešení i při reálném multimediálním zatížení.

„Šifrátor během testů prokázal schopnost využít plnou kapacitu 100 Gb/s linky při přenosu velkých datových rámců. Reálně dosažené rychlosti byly omezeny především výkonem použitého generátoru provozu, nikoliv samotným šifrovacím systémem,“ vysvětluje Ondřej Havliš ze sdružení CESNET.

Výsledky: připravenost pro praktické nasazení
Testy v reálném provozu ukázaly, že propojení QKD a postkvantové kryptografie dokáže spolehlivě zabezpečit i velmi rychlé datové přenosy. V praxi to znamená, že tato technologie je připravena chránit kritické síťové služby – a to i tam, kde jsou kladeny vysoké nároky na kapacitu a stabilitu. Kombinace QKD a PQC tak představuje robustní a prakticky použitelné řešení pro síťové aplikace, které vyžadují nejvyšší úroveň zabezpečení.

https://www.cesnet.cz/novinky/kvantove-zabezpeceny-prenos-na-100-gb-s-v-realne-siti-292