Universitas Mercatorum

Università telematica delle Camere di Commercio Italiane

NOME PROGETTO

Sicurezza e Autenticazione mediante Firma Elettro/ottica (SAFE)

P.I.

Prof. Luca Potì

CODIFICA

15-FIN/RIC

CLASSE FINANZIAMENTO

Avanzato

FASCIA

Ordinario

S.S.D.

ING-INF/03

GSD

09/IINF-03

S.C.

09/F2

STRUTTURA AFFERENZA

Facoltà di Scienze Tecnologiche e dell'Innovazione, Università Telematica Universitas Mercatorum

OBIETTIVI PROGETTO DI RICERCA

Il principale obiettivo del progetto SAFE è lo **studio di fattibilità** per una tecnica in grado di incrementare **la sicurezza all'interno di una rete ottica o di un semplice sistema di trasmissione ottico** a livello fisico, garantendo identificazione, autenticazione, sicurezza del dato trasmesso e monitoraggio. La tecnica proposta si basa sull'assunzione che ogni elemento fisico abbia la sua impronta digitale. Ciò che si propone è una modalità operativa per leggere tale impronta, confrontarla con quella attesa (nota) per confermare l'autenticità della stessa. Si utilizzerà la misura del segnale retrodiffuso generato da ogni fibra ottica. A tale scopo vengono individuati obiettivi secondari che, nella durata del progetto, consentiranno di verificare le potenzialità delle tecniche proposte.

1. **Implementazione del modello teorico**

La prima e fondamentale operazione sarà quella di fornire un modello teorico che descriva la fenomenologia (Rayleigth backscattering) che dovrà quindi essere poi tradotto in un codice numerico in grado di emulare le diverse operazioni necessarie.

2. **Studio numerico**

Lo strumento sviluppato nell'obiettivo precedente consentirà di simulare, in modo estensivo, la generazione del segnale retrodiffuso, la trasformazione in firma digitale ed una valutazione di verosimiglianza mediante lo studio della distanza di Hamming per il caso di segnali binari e la distanza vettoriale per segnali non binari.

3. **Definizione delle specifiche per un collegamento sicuro intra ed inter aziendale**

I casi applicativi saranno quelli di un collegamento sicuro all'interno di una azienda o tra aziende diverse. Per queste verranno delineate le specifiche in termini di distanza dei collegamenti, di probabilità di corretta identificazione e di contraffazione.

4. **Progettazione del sistema**

I casi di studio saranno progettati, elencandone gli elementi costituenti e le relative interconnessioni.

5. **Dimostrazione di fattibilità**

Risultati numerici dimostreranno l'efficacia della tecnica proposta e la possibilità di implementazione pratica.

RISULTATI RAGGIUNTI

La ricerca ha prodotto numerosi risultati, elencati di seguito.

- La definizione della firma con bit assicura una probabilità di errore molto basse in numerosi scenari, stimata con un approccio semianalitico usando la distanza di Hamming.
- Definizione di un'architettura di transceiver (TRX) in grado di trasmettere dati e eseguire l'identificazione di un sistema ottico, mostrata in Figura 1. La sicurezza del sistema è stata misurata in termini di probabilità di falso negativo e falso positivo, raggiungendo valori

molto bassi con requisiti di sistema ottenibili con costi bassi, come mostrato nelle Figure 2(a)(b).

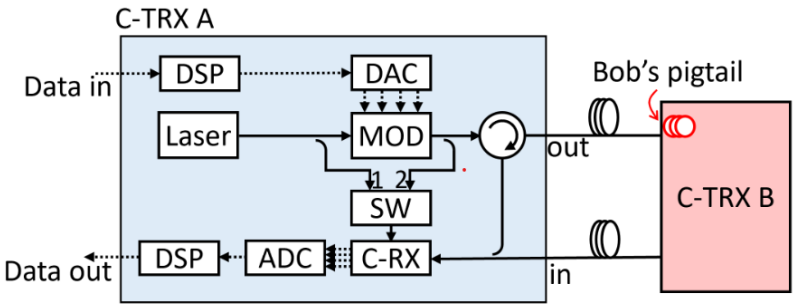

Figura 1 Architettura di trasmissione. C-TRX A può sia trasmettere informazione che identificare C-TRX B attraverso il suo pigtail usando la C-OFDR.

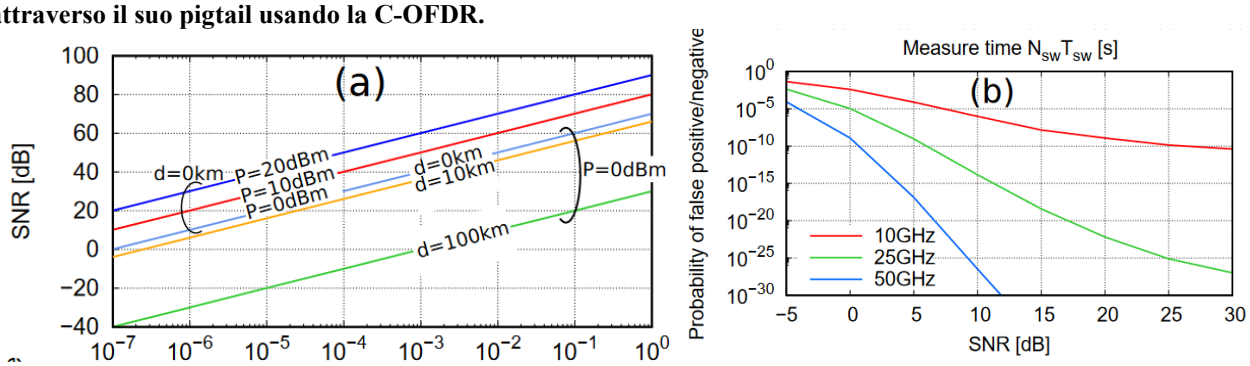

Figura 2: (a) SNR sulla firma rispetto al tempo di misura e (b) probability di falso positivo e falso negativo rispetto all'SNR in un sistema punto-punto.

- La dispersione ha un impatto molto forte sulla firma, che può essere compensato solo in parte. Allo stato attuale, conviene usare la tecnica proposta in scenari senza dispersione, ad esempio fibre senza dispersione, oppure compensandola con fibre dispersion-shifted.
- La banda richiesta per gli strumenti usati per la misura di identificazione ottica può essere sufficientemente piccola (<50GHz) e dunque si può facilmente ottenere con dispositivi commerciali e a basso costo.
- Definizione di un protocollo per l'identificazione ottica di sottosistemi in una rete in uno scenario intra-aziendale (1km) e in uno inter-aziendale (30km). I risultati sono mostrati in Figura 3(a)(b).

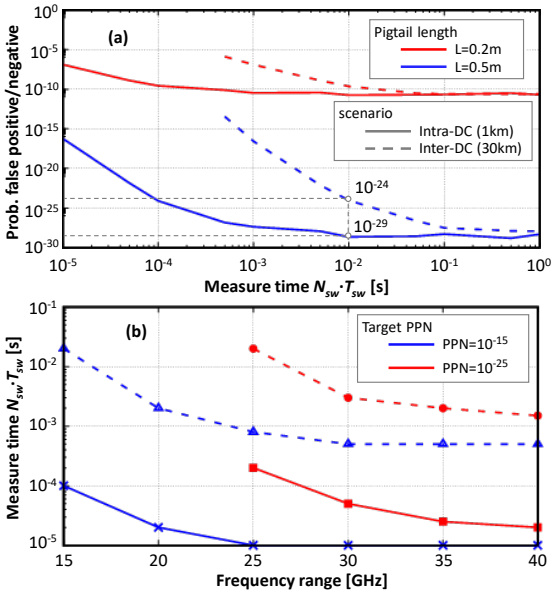

Figura 3 (a) probabilità di falso negativo e positivo rispetto al tempo di misura e (b) tempo di misura richiesto per probabilità di falso positivo e negativo (PPN) fissata, rispetto alla banda richiesta.

PRODOTTI DELLA RICERCA

Partecipazione a convegni internazionali

1. "Coherent transceiver architecture enabling data transmission and optical identification", S. Civelli, M. Secondini, P. Nadimi Goki, L. Potì accepted for presentation at the IEEE Summer Topical meeting and Photonics in Switching (PSC) conference 2024 to be held in July in Barbados.
2. "System architecture for optical identification in amplified optical networks" S. Civelli, M. Secondini, P. Nadimi Goki, L. Potì, submitted to the European conference on optical communication (ECOC) 2024.
3. "Optical identification: a new paradigm in physical layer security", N. Andriolli, R. Caldelli, S. Civelli, P. Nadimi Goki, T. T. Mulugeta, N. Sambo, M. Secondini, L. Potì, ONDM 2024, Workshop
4. "What if optical sub-systems had a signature?" S. Civelli the IEEE Summer Topical meeting and Photonics in Switching (PSC) conference 2024 to be held in July in Barbados.

Elementi per il consolidamento

1. "Optical identification for enhanced-security SDM and Multi-Band networks", L. Potì, IEEE Summer Topical meeting and Photonics in Switching (PSC) conference 2024 to be held in July in Barbados.
2. Journal paper in preparation, to be submitted to the Journal of Optical Communication and Networking