Physical Layer Security: tecnologie e applicazioni

Simone Soderi

Sommario

Viviamo in una società iperconnessa dove le tecnologie di comunicazione ci supportano nelle attività quotidiane. In una visione olistica della sicurezza di questo vasto cyber-spazio merita approfondire il ruolo della Physical Layer Security (PLS) e delle sue applicazioni in diverse aree di comunicazione. L'obiettivo di questo articolo è delineare le sfide attuali nel campo della sicurezza delle reti e introdurre la PLS come un approccio diverso e complementare ai tradizionali meccanismi di sicurezza di cui condividono l'obiettivo di garantire la sicurezza delle comunicazioni. A livello fisico, per garantire la sicurezza dei dati trasmessi la PLS sfrutta le proprietà uniche dei canali di comunicazione o le tecniche di watermarking e jamming, su cui porremo qui particolare enfasi. Presenteremo diverse applicazioni della PLS, tra cui le comunicazioni acustiche, le comunicazioni veicolari e le comunicazioni su onde luminose per le reti 6G evidenziando le peculiarità specifiche della PLS in contesti specifici e i relativi vantaggi. Sebbene ci siano già casi d'uso in cui la PLS è stata applicata con successo, è fondamentale guidare la ricerca per sviluppare soluzioni adatte alle reti di nuova generazione.

Abstract

We live in a hyper-connected society where communication technologies support our daily activities. In a holistic view of the security of this vaste cyber-space, it is worth exploring the role of Physical Layer Security (PLS) and its applications in different areas of communication. This article outlines the current challenges in network security and introduce PLS as a different and complementary approach to conventional security mechanisms sharing the goal of securing communications PLS guarantees the security of transmitted data at the physical level, by exploiting unique properties of communication channels, or watermarking and jamming techniques. We will also emphasize PLS applications that utilize watermarking and jamming as security implementations. Next, several applications of PLS are explored, including acoustic communications, vehicular communications, and lightwave communications for 6G networks. This review of real-life applications highlights the specific peculiarities of PLS in specific contexts and their advantages. Although there are already use cases where PLS has been successfully applied, it is crucial to drive research to develop solutions suitable for next-generation networks.

Parole chiave

Physical layer security (PLS) (sicurezza a livello fisico), 6G, sicurezza, watermarking (filigrana), jamming (interferenza).

1 Introduzione

Le infrastrutture di comunicazione possono essere descritte con un modello organizzato per livelli. Tale paradigma intende caratterizzare le funzioni fondamentali di una rete di comunicazione su livelli diversi che comunicano tra di loro per mezzo di specifiche interfacce. Queste funzioni prevedono ad esempio la trasmissione, l'instradamento, l'allocazione delle risorse, l'affidabilità e il controllo della congestione dei protocolli, fino all'applicazione finale; ognuno di questi livelli ha strumenti e astrazioni di rete specifici. I modelli di riferimento sono il modello Open System Interconnection (OSI) ed il modello TCP/IP [2] (vedi Figura 1). Entrambi

questi modelli hanno mostrato la loro efficacia per descrivere il funzionamento delle reti, e da molti anni sono usati anche per lo studio della sicurezza delle reti.

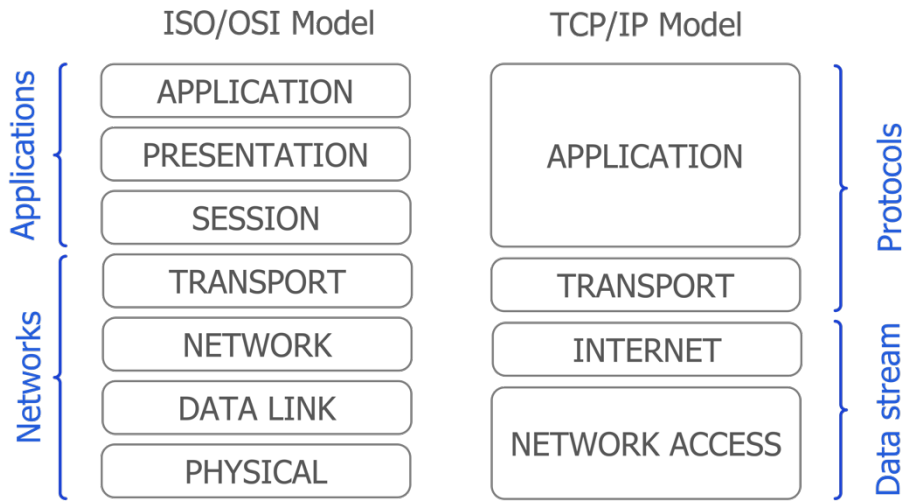

Figura 1 - Modelli di riferimento per descrivere le reti di comunicazione e i loro componenti.

Nei primi giorni di Internet, la *sicurezza* non era considerata una priorità a causa dell'accesso limitato e controllato alle reti. Tuttavia, con l'aumento delle connessioni, la proliferazione delle applicazioni e la diffusione delle comunicazioni wireless, la sicurezza delle reti è diventata una questione sempre più urgente. In risposta a ciò, sono state sviluppate soluzioni tecniche come il controllo degli accessi, p.e. tramite password, e la crittografia end-to-end. Tuttavia, la pratica di aggiungere autenticazione e crittografia ai protocolli esistenti ai vari livelli di comunicazione ha causato un mosaico di meccanismi di sicurezza.
La costante crescita della connettività in ogni settore ha portato a una consapevolezza senza precedenti dell'importanza della sicurezza di rete in tutte le sue forme. Nonostante ciò, il livello fisico della pila di protocolli (Figura 1) è rimasto a lungo poco esplorato nel panorama della sicurezza delle comunicazioni. Questo livello si trova all'estremità inferiore della stack protocollare e essenzialmente converte i bit di informazione in segnali modulati adatti al canale di comunicazione scelto.

Questa minore popolarità del livello fisico per fare sicurezza è sorprendente, infatti la stocasticità stessa che i canali fisici di comunicazione offrono per loro stessa natura è spesso alla base della generazione e distribuzione delle chiavi dei sistemi di segretezza. Queste osservazioni stanno alla base di varie soluzioni di *sicurezza a livello fisico* (nel resto dell'articolo useremo anche il termine *Physical Layer Security (PLS)*). Tali tecnologie ambiscono a fornire sicurezza in modo autonomo operando al solo livello fisico dell'architettura del protocollo di comunicazione usato.

L'assenza di un approccio universale alla PLS può essere in parte spiegata da come vengono spesso presentate e insegnate le questioni di sicurezza. I corsi in crittografia e sicurezza spesso iniziano con una discussione sulla nozione di perfetta segretezza di Shannon [3], ma poi la sicurezza teorica dell'informazione viene considerata irrealizzabile in pratica. Invece, vengono proposti algoritmi di crittografia che non sfruttano le caratteristiche del canale di comunicazione essendo basati su operazioni matematiche ritenute difficili da calcolare, come la fattorizzazione dei primi.
È invece ragionevole sostenere che le misure di sicurezza dovrebbero essere implementate a tutti i livelli, laddove sia possibile farlo in modo economicamente vantaggioso [9] perché la

sicurezza fisica può essere un'importante risorsa per migliorare la sicurezza globale di una rete. Questo è particolarmente vero per le reti wireless, dove la trasmissione radio è influenzata da molti fattori esterni, come le interferenze, la propagazione del segnale, il multipath fading[1] e l'attenuazione del segnale. Come abbiamo già detto questi fattori possono essere sfruttati per l'implementazione di tecniche di sicurezza nel livello fisico. Ad esempio, l'analisi delle caratteristiche del canale può essere utilizzata per la generazione di chiavi crittografiche, per l'autenticazione dei dispositivi e per mitigare attacchi.

La sicurezza dei dati è un aspetto cruciale nella progettazione delle reti di comunicazione e la sicurezza fisica può fungere da risorsa chiave per migliorare l'affidabilità globale di una rete. Integrando le tecniche di sicurezza fisica con le tradizionali tecniche crittografiche, è possibile creare un sistema di comunicazione resiliente e affidabile, in grado di resistere a un'ampia gamma di attacchi e adattarsi alle nuove minacce emergenti. Questo articolo si propone di evidenziare l'importanza della sicurezza fisica nella progettazione delle reti di comunicazione e fornisce una panoramica delle tecniche basate sulle caratteristiche del canale di comunicazione, valutando i vantaggi e gli svantaggi rispetto alle tradizionali tecniche di sicurezza. Tuttavia, l'integrazione di soluzioni PLS nelle reti di comunicazione presenta tuttora sfide significative che richiedono un'attenta progettazione e implementazione dei futuri sistemi. È fondamentale sviluppare dispositivi in grado di implementare in modo efficace, scalabile ed efficiente energeticamente questo nuovo paradigma per la sicurezza delle comunicazioni.

2 Fondamenti della sicurezza a livello fisico

In questa sezione vogliamo fornire alcuni concetti chiave per poter comprendere come possiamo inquadrare la PLS nel panorama della sicurezza tradizionale. Verranno inoltre descritte le principali metriche utilizzate per descrivere e valutare la PLS. Infine, tratteremo alcune tecniche usate per l'implementazione della sicurezza a livello fisico.

2.1 Crittografia e sicurezza a livello fisico

La crittografia rappresenta il nucleo fondante dell'arte di codificare e decodificare le informazioni, avendo le sue radici in tempi antichi quando la necessità di mantenere segrete le comunicazioni si scontrava con le limitate tecnologie disponibili. I sistemi crittografici si basano su tecniche di sostituzione e trasposizione dei caratteri, creando un testo cifrato che può essere decodificato solo conoscendo la chiave o il metodo specifico utilizzato per la cifratura. Tra gli esempi più famosi di crittografia classica figurano il cifrario di Cesare, usato nell'antica Roma, e il cifrario Enigma, utilizzato dalla Germania durante la Seconda Guerra Mondiale. Sebbene queste tecniche siano state sostanzialmente superate dal progresso tecnologico e dalla crittografia moderna, che sfrutta principi matematici complessi e algoritmi avanzati (ad esempio, Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Elliptic Curve Cryptography (ECC)), l'importanza della crittografia rimane ineguagliabile per la sua influenza storica e per la sua fondamentale introduzione di concetti chiave come la chiave crittografica e l'uso di algoritmi per la codifica delle informazioni.

[1] Il **multipath fading** è una forma di distorsione di un segnale che giunge a destinazione sotto forma di un certo numero di repliche, sfasate nel tempo, originate dai percorsi multipli (*multipath*) che il segnale stesso può aver seguito durante la sua propagazione. Percorsi che vengono generati da ostacoli che il segnale trasmesso incontra prima di arrivare al ricevitore.

Nel 1949, il matematico e ingegnere statunitense Claude Shannon ha introdotto il concetto di "sicurezza perfetta" [3]. Secondo Shannon, un sistema crittografico raggiunge una sicurezza perfetta (o perfetta segretezza) se la probabilità a posteriori di conoscere il testo in chiaro, avendo osservato il testo cifrato, è la stessa della probabilità a priori. In altre parole, l'avversario non può ottenere alcuna informazione sul testo in chiaro osservando il testo cifrato.

Shannon ha definito un sistema che opera in perfetta segretezza se l'informazione mutua[2] (I) tra il messaggio $(x_S)^N$, composto da N bit[3], e l'uscita del codificatore $(x_S{}')^N$, anche esso composto da N bit, è pari a zero. Formalmente:

$$I((x_S)^N; (x_S{}')^N) = 0.$$

Un esempio pratico di un sistema crittografico che raggiunge la sicurezza perfetta è il cifrario "one-time pad". Questo sistema utilizza una chiave di cifratura generata casualmente che ha la stessa lunghezza del messaggio da cifrare. Il principio di funzionamento è semplice: la chiave viene utilizzata una sola volta per cifrare e decifrare il messaggio. Se la chiave viene generata in modo completamente casuale, mantenuta segreta e utilizzata solo una volta, allora il cifrario one-time pad è inattaccabile.

In molte applicazioni non siamo interessati ad una sicurezza perfetta ma può essere sufficiente che un sistema non venga compromesso da un attaccante in un tempo ragionevole oppure con una ragionevole probabilità di successo. In questi casi stiamo utilizzando un approccio alla sicurezza di tipo *computazionale* (vedere il "Riquadro 1: Valutazione della sicurezza di un sistema crittografico" per i criteri di valutazione di un sistema crittografico).

Tuttavia, il modello di sicurezza computazionale presenta alcuni svantaggi. La sicurezza della crittografia a chiave pubblica si basa sulla congettura che alcune funzioni unidirezionali siano difficili da invertire, una supposizione che rimane nondimeno matematicamente non dimostrata. E' altrettanto vero che la potenza di calcolo continua a crescere rapidamente, rendendo gli attacchi di forza bruta, un tempo considerati irrealizzabili, sempre più fattibili.

La protezione dei dati in transito da accessi non autorizzati è un aspetto fondamentale delle comunicazioni in una rete. I protocolli crittografici soddisfano questa esigenza consentendo solo a chi possiede le credenziali appropriate di interpretare il protocollo. Tuttavia, in alcuni casi la crittografia tradizionale potrebbe non essere sufficiente oppure potrebbe non essere efficiente (pensiamo, ad esempio, al caso di dispositivi Internet of Things (IoT) che hanno limitate capacità computazionali), e per tale motivo da molti anni si è iniziato ad esplorare metodi alternativi che possono comunque rendere le comunicazioni sicure.
Le tecniche basate sulla PLS mirano a garantire la sicurezza dei dati trasmessi, ad esempio tra i sensori senza fili e il sistema centrale, attraverso l'*elaborazione digitale del segnale* inviato prima della sua trasmissione sul mezzo di comunicazione scelto e utilizzando alcune proprietà fisiche del canale di comunicazione. La PLS può offrire, in prospettiva, le stesse proprietà di sicurezza senza dover ricorrere a protocolli eseguiti a livelli superiori a quello fisico.

[2] Nella teoria della probabilità e dell'informazione, l'informazione mutua (I) di due variabili casuali è una misura della dipendenza reciproca tra le due variabili. Più specificamente, quantifica la "quantità di informazioni" (ad esempio in unità come i bit) ottenute su una variabile casuale osservando l'altra variabile casuale.
[3] Il bit è stato definito da Shannon come la quantità di informazione necessaria, e sufficiente, per discriminare e decidere tra due soli eventi equiprobabili.

Esistono notevoli differenze tra i principi crittografici classici impiegati nei livelli più alti della pila protocollare e la sicurezza a livello fisico basata sui principi della teoria dell'informazione; pertanto, è fondamentale comprendere queste differenze e come esse influiscono sulla scelta della tecnologia in contesti pratici.

Nonostante la sua potenza concettuale, il problema delle comunicazioni sicure si riduceva al problema della distribuzione sicura delle chiavi, e si credeva ampiamente che la segretezza perfetta, per esempio usando il "one-time pad", non fosse raggiungibile nei sistemi pratici.
La sicurezza basata sulla teoria dell'informazione definita da Shannon è stata ulteriormente estesa dal lavoro fondamentale di Wyner con il cosiddetto canale *wiretap* [4] e dalle successive generalizzazioni di Csiszár e Körner [5].
Il modello di canale wiretap di Wyner ipotizza che una comunicazione sicura può essere ottenuta quando l'attaccante riceve una versione degradata del segnale trasmesso. Ovvero, come mostrato in Figura 2, quando il canale di comunicazione principale (i.e., il *main channel* che collega Alice, il mittente, e Bob, il destinatario) è migliore in termini di rapporto segnale rumore (SNR) rispetto al canale indipendente (i.e., il *wiretap channel* tra Alice e Eve) verso l'attaccante.
La Figura 2 mostra un modello di canale wiretap non degradato che include un trasmettitore, cioè Alice, un ricevitore legittimo Bob e Eve un attaccante passivo (eavesdropper).

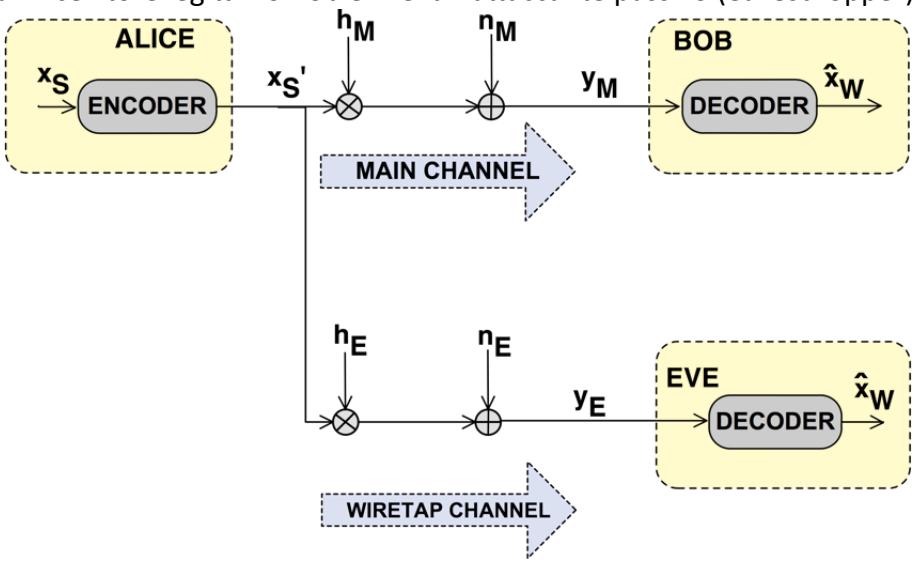

Figura 2 – Modello di canale wiretap proposto da Wyner.

Insieme all'introduzione del canale di intercettazione (i.e., wiretap), Wyner ha suggerito l'utilizzo della *segretezza debole*, in cui la quantità di informazioni trapelate sul messaggio $(x_S)^N$ da parte dell'attaccante quando osserva $(y_E)^N$, è asintoticamente pari a 0, vale a dire,

$$\lim_{N\to\infty} \frac{1}{N} I((x_S)^N; (y_E)^N) = 0.$$

Alcune applicazioni non possono però accettare alcuna perdita di informazioni e così nel 2000 Maurer *et al.* [6] hanno definito la *segretezza forte* come segue

$$\lim_{N\to\infty} I((x_S)^N; (y_E)^N) = 0.$$

La segretezza forte è difficile da progettare, mentre la segretezza debole conserva un interesse pratico. Ricordiamo che la capacità di segretezza (C_S) del collegamento legittimo è definita come la massima quantità di bit scambiati in modo sicuro e descritta dalla seguente equazione

$$C_S = max(0, C_B - C_E).$$

In altre parole, C_s è rappresentata dalla capacità del canale tra Alice e Bob (C_B) meno tutti i bit che possono essere letti dall'attaccante e quindi rappresentati dalla capacità del canale tra Alice e Eve (C_E). L'obiettivo della sicurezza del livello fisico è quello di implementare una comunicazione sicura e affidabile tra Alice e Bob, garantendo un specifica capacità di segretezza. Nel caso in cui la capacità di segretezza si riduca a 0, e questo accade quando il l'attaccante ha un buon canale di comunicazione verso il trasmettitore legittimo, Alice può decidere di non trasmettere, evitando così di rivelare qualsiasi informazione.

È importante notare che l'approccio crittografico classico è in contrasto con il meccanismo introdotto dalla sicurezza del livello fisico. In genere, la solidità del meccanismo di sicurezza della crittografia si basa sul rigore della matematica e sul modo in cui gli utenti mantengono le chiavi segrete, mentre la sicurezza del livello fisico garantisce la sicurezza delle comunicazioni sfruttando delle caratteristiche del canale. Un risultato importante nell'ambito della sicurezza del livello fisico è l'implementazione che sfrutta le informazioni imperfette sullo stato del canale (CSI).

I principali vantaggi della sicurezza a livello fisico nel contesto del modello di sicurezza teorico dell'informazione risiedono nell'assenza di restrizioni computazionali sull'attaccante e nella possibilità di fare affermazioni precise sulle informazioni divulgate all'attaccante in base alla qualità del canale.
Tuttavia, ci sono anche alcuni svantaggi da considerare. Prima di tutto, la sicurezza teorica dell'informazione si basa su misure medie di informazione. Il sistema può essere progettato e ottimizzato per un determinato livello di sicurezza, affermando ad esempio che è possibile garantire una determinata C_s con una certa probabilità (tipicamente definita come "probabilità di blocco"); tuttavia, potrebbe non essere possibile garantire la riservatezza con probabilità pari a 1. Inoltre, siamo costretti a fare ipotesi sui canali di comunicazione che potrebbero non essere accurate nella pratica. Nella maggior parte dei casi, le ipotesi sui canali sono molto conservative, il che potrebbe comportare bassa capacità di segretezza.

Alla luce di queste considerazioni, possiamo dire che per rendere una comunicazione sicura si possono anche studiare soluzioni basate su più livelli, in cui le varie proprietà di sicurezza (confidenzialità, integrità e autenticità) possono essere implementate in punti diversi del modello OSI a seconda dell'applicazione o del caso d'uso. Questo approccio modulare offre quindi una ulteriore opportunità per migliorare la sicurezza delle moderne reti di comunicazione anche attraverso l'utilizzo della sicurezza a livello fisico.

2.2 Tecniche di PLS

Esistono diverse tecniche che possono essere impiegate per implementare la sicurezza a livello fisico (PLS). Tra le tecniche più comunemente utilizzate è importante ricordare:

- **Codifica di modulazione sicura:** Questa tecnica combina la codifica di canale e la modulazione per introdurre un elevato livello di sicurezza nella trasmissione dei dati. La codifica aggiunge ridondanza e complessità ai segnali trasmessi, rendendo più difficile per un potenziale attaccante decodificare correttamente i dati senza conoscere gli algoritmi di codifica specifici. La modulazione può essere adattiva, in modo che il tipo di modulazione utilizzata varia in modo casuale o dinamico nel tempo, rendendo ancora più difficile l'intercettazione del segnale.

- **Beamforming:** Nel contesto delle comunicazioni radio e mediante onde luminose (Visible Light Communication (VLC)), il beamforming *sicuro* sfrutta l'uso di antenne multiple per concentrare il segnale trasmesso in una specifica direzione spaziale, conosciuta solo al destinatario legittimo. Questa tecnica rende più difficile per un attaccante intercettare il segnale o interferire con la comunicazione, in quanto il segnale è direzionato in modo specifico e potrebbe non essere rilevato o decodificato correttamente da un'antenna posizionata altrove.

- **Selezione del canale:** La selezione del canale sicura sfrutta le caratteristiche del canale radio per scegliere canali sicuri per la trasmissione dei dati. Vengono valutati i parametri del canale, come la qualità del segnale, il rapporto segnale-rumore e la presenza di interferenze. Sulla base di queste valutazioni, vengono selezionati i canali che offrono una buona qualità e una bassa probabilità di intercettazione o interferenza. Ciò aiuta a garantire la sicurezza della comunicazione utilizzando canali più affidabili.

- **Generazione di chiavi da casualità del canale:** Questa tecnica sfrutta le proprietà casuali del canale stesso per generare chiavi di crittografia sicure. Gli algoritmi estraggono informazioni casuali dal segnale trasmesso, ad esempio campionando il rumore presente nel canale o analizzando le variazioni spazio-temporali delle caratteristiche del segnale. Queste informazioni casuali vengono quindi utilizzate come base per generare le chiavi di crittografia, garantendo che siano uniche e imprevedibili.

- **Criptazione basata su rumore:** Questa tecnica sfrutta l'aggiunta intenzionale di rumore al segnale trasmesso. Il rumore può essere generato in modo casuale o utilizzando algoritmi specifici. Solo il destinatario legittimo, che conosce i dettagli della trasmissione, può rimuovere correttamente il rumore e ricostruire i dati originali. La criptazione basata su rumore rende più difficile per un attaccante intercettare e decodificare correttamente i dati, in quanto il rumore aggiunto introduce incertezza nella trasmissione.

- **Codici di cancellazione dell'interferenza:** Questi codici vengono utilizzati per mitigare l'interferenza causata da segnali indesiderati o attaccanti. Consentono al ricevitore di isolare il segnale desiderato e rimuovere o mitigare l'interferenza. L'uso di algoritmi di elaborazione del segnale permette di analizzare il segnale ricevuto, identificare e cancellare le componenti di interferenza, migliorando così la qualità e la sicurezza della comunicazione.

Queste tecniche rappresentano una panoramica delle possibili metodologie utilizzate per implementare la PLS in ambito radio e VLC. La scelta e l'implementazione delle tecniche dipendono dalle specifiche esigenze di sicurezza del sistema e dalle caratteristiche del canale di comunicazione utilizzato.

2.3 Considerazioni sulla sicurezza basata sulla diversità del canale

Nel contesto della sicurezza delle comunicazioni digitali, spesso si ricorre a soluzioni complesse come password intricate o sofisticati sistemi di cifratura. Tuttavia, esiste un approccio meno convenzionale che trae vantaggio da un aspetto molto più naturale e variabile: le differenze nella qualità dei canali di comunicazione utilizzati. I messaggi di solito

subiscono interferenze che variano da un punto di trasmissione all'altro e le tecniche proposte sfruttano proprio questa caratteristica. L'idea di fondo è quella di usare le distorsioni casuali e le fluttuazioni - comunemente denominate "rumore" - che affliggono ogni sistema di comunicazione wireless come sorgente per la creazione di chiavi crittografiche condivise tra le entità comunicanti.

In questo contesto, il processo di estrazione delle chiavi si articola in diverse fasi:

1. **Osservazione congiunta del rumore:** In un sistema di comunicazione wireless, due entità (ad esempio, due dispositivi della rete di comunicazione) sono sottoposte a livelli simili di interferenze e rumori ambientali. Queste perturbazioni, pur essendo intrinsecamente casuali e imprevedibili, mantengono una certa correlazione quando osservate da entrambe le entità entro una vicinanza spaziale definita.
2. **Derivazione di sequenze aleatorie:** Le due entità, mediante un processo sincronizzato, campionano e analizzano il rumore ambientale percepito sul canale di comunicazione ed estraggono sequenze di dati che, come detto, presentano elevati livelli di correlazione. Queste sequenze fungono da basi per la generazione delle chiavi crittografiche.
3. **Generazione della chiave crittografica:** Successivamente, le sequenze casuali vengono trasformate attraverso specifici algoritmi (noti in letteratura e condivisi a priori tra le due entità) in una serie uniforme di bit. Questa serie di bit, ottenuta indipendentemente da ciascuna delle due entità ma risultante identica per entrambe, costituisce la chiave crittografica condivisa, conosciuta soltanto ai dispositivi che hanno partecipato alla sua generazione.

Si deve notare che l'efficacia di questo approccio è soggetta a determinati prerequisiti e fattori. La qualità e l'affidabilità del segnale campionato per la generazione delle chiavi sono di vitale importanza; infatti un canale eccessivamente affetto da rumore potrebbe inficiare la qualità della chiave e, di conseguenza, la sicurezza della comunicazione. Inoltre, la variabilità temporale e spaziale del canale wireless richiede che gli algoritmi di generazione delle chiavi siano sufficientemente robusti da adattarsi a tali fluttuazioni, per garantire la continuità e l'affidabilità del meccanismo di sicurezza implementato.

La generazione di chiavi dal rumore del canale rappresenta, pertanto, un approccio innovativo e complementare ai tradizionali sistemi di creazione e scambio delle chiavi, offrendo una soluzione integrata e dinamica per la sicurezza nelle comunicazioni wireless. Infatti esso non richiede né un algoritmo sofisticato e un'entità che generi le chiavi, né un protocollo e un canale dedicato alla loro distribuzione. Tuttavia, la sua realizzazione pratica richiede un'attenta considerazione delle dinamiche del canale e delle capacità di elaborazione dei dispositivi, oltre allo sviluppo di algoritmi specifici per la gestione e l'estrazione efficace delle informazioni casuali necessarie alla creazione di chiavi crittografiche affidabili e sicure.

2.4 Soluzioni di sicurezza basate su Reconfigurable Intelligent Surface (RIS)

Nelle tecnologie di comunicazione tradizionali, le proprietà di propagazione dei canali wireless non possono essere controllate in modo adattivo per ottenere la desiderata sicurezza della comunicazione. Per tale motivo, negli ultimi anni, la sicurezza a livello fisico realizzata usando superfici riflettenti intelligenti (Reflective Intelligent Surface (RIS)) è emersa come una promettente tecnologia per migliorare le comunicazioni wireless in termini di efficienza energetica e spettrale [10]. I RIS possono essere utilizzati sia nelle comunicazioni a radiofrequenza che nelle comunicazioni basate sulla luce visibile (VLC).

Nel contesto delle comunicazioni a radiofrequenza, il RIS è costituito da elementi riflettenti a basso costo che possono essere progettati come una matrice di riflessione passiva programmabile. I segnali trasmessi dalla stazione di base vengono riflessi dal RIS per migliorare la copertura mobile e la qualità di trasmissione. Grazie alla capacità di manipolare selettivamente i segnali riflessi, il RIS può essere utilizzato anche per implementare meccanismi di sicurezza a livello fisico, sfruttando ad esempio la diversità spaziale o la generazione di chiavi crittografiche.

Nel contesto delle comunicazioni basate sulla luce visibile, i RIS ottici possono essere realizzati mediante l'utilizzo di metasuperfici o matrice di specchi. Questi elementi consentono di controllare in modo attivo la propagazione della luce, migliorando la copertura e la qualità del segnale. L'utilizzo dei RIS ottici nelle VLC offre l'opportunità di migliorare la sicurezza a livello fisico mediante l'implementazione di tecniche come la modulazione del segnale, l'ottimizzazione della direzionalità del segnale (verso il ricevitore legittimo) e la gestione del canale di comunicazione.
I RIS offrono anche importanti vantaggi per le implementazioni pratiche. Ad esempio, gli elementi riflettenti del RIS riflettono passivamente i segnali in ingresso senza richiedere operazioni sofisticate di elaborazione del segnale che richiedono hardware trasmittente a radio frequenza. Pertanto, rispetto ai trasmettitori attivi convenzionali, i RIS ottici potranno operare a un costo molto inferiore in termini di hardware e consumo energetico. Inoltre, grazie alla natura passiva degli elementi riflettenti, i RIS possono essere realizzati in modo da avere un peso leggero e uno spessore limitato, rendendoli così facilmente installabili su pareti, soffitti, cartelli, lampioni, e così via. Infine, un RIS opera naturalmente in modalità full-duplex senza auto-interferenza o introduzione di rumore termico [11].

Nonostante l'analisi della capacità di segretezza sia stata affrontata in lavori esistenti nel contesto dei RIS, esistono ancora sfide aperte per implementare soluzioni PLS basate su RIS. Tali sfide includono i materiali per realizzare queste di metasuperfici intelligenti e la loro integrazione all'interno dei dispositivi di trasmissione e ricezione.

2.5 Sicurezza basata watermarking e il jamming

Esistono molti modi per implementare la sicurezza a livello fisico; è possibile farlo sfruttando la variabilità del canale di comunicazione oppure attraverso la cooperazione tra nodi della stessa rete per creare un'interferenza tale da degradare il canale dell'attaccante. In questa sezione vogliamo parlare di un approccio diverso che si basa su tecniche sviluppate negli ultimi anni che implementano la PLS attraverso l'elaborazione numerica dei segnali.

Nel 2017 Soderi *et al*. [7] hanno mostrato come è possibile utilizzare watermarking e jamming per implementare la sicurezza a livello fisico nelle comunicazioni. L'approccio denominato Watermarked Blind Physical Layer Security (WBPLSec), combina queste due tecniche in modo complementare per proteggere la trasmissione dei dati e garantire la riservatezza e l'integrità delle informazioni.

Il watermarking si basa sull'inserimento segreto di informazioni aggiuntive (il watermark o filigrana) nel segnale trasmesso, visibili solo all'unico destinatario legittimato a ricevere l'informazione trasmessa. Questo si realizza attraverso l'uso di modulazioni a spettro espanso (i.e., Spread-Spectrum (SS) vedi Riquadro 2: Tecnologia a spettro espanso) per camuffare il watermark all'interno del segnale originale, senza alterare le informazioni portate.

Il jamming, invece, è una tecnica di interferenza intenzionale che disturba la trasmissione dei dati rendendo difficile per un attaccante ascoltare o decifrare il segnale trasmesso. Secondo quanto proposto con WBPLSec, un ricevitore legittimo (ovvero colui che è l'unico destinatario dell'informazione trasmessa) può essere progettato per compensare l'effetto del jamming e recuperare il segnale originale utilizzando il watermark.
Combinando queste due tecniche, è possibile creare una *regione di sicurezza* attorno al ricevitore legittimo, garantendo comunicazioni con un alto grado di riservatezza in determinate condizioni. Il watermarking e il jamming possono essere applicati in diversi contesti, tra cui comunicazioni wireless, comunicazioni acustiche e comunicazioni nelle reti di nuova generazione (6G).
Tuttavia, è importante notare che l'efficacia di queste tecniche dipende dalle specifiche del sistema di comunicazione e dalle condizioni di trasmissione. Ad esempio, affinché il jamming sia efficace, il canale di comunicazione deve consentire interferenze intenzionali nella trasmissione dei dati, e i nodi ricevitori della rete devono essere dotati di almeno un trasmettitore e un ricevitore che possano essere utilizzati contemporaneamente.
Il processo innovativo per implementare la sicurezza a livello fisico alla base del WBPLSec è composto dai seguenti passaggi:

1. **Watermarking a spettro espanso**: il segnale trasmesso da Alice contiene un messaggio che viene prima modulato con una sequenza che espande lo spettro. In questo modo, il segnale originale a banda stretta viene marchiato con il watermark a spettro espanso.
2. **Ricevitore jamming**: Bob, il ricevitore con jamming, interferisce solo con una parte del segnale ricevuto. Poiché Bob conosce quali campioni sono stati disturbati, è in grado di ricostruire un simbolo pulito.

3 Esempi di applicazioni della sicurezza a livello fisico

3.1 Domini di applicazione di WBPLSec

L'applicazione del WBPLSec è soggetta al rispetto di alcuni requisiti. Per applicare il jamming, è necessario che il canale di comunicazione supporti interferenze intenzionali durante la trasmissione dei dati. Questa condizione viene soddisfatta dalla maggior parte dei canali di comunicazione condivisi in cui le trasmissioni possono entrare in collisione. Un altro requisito tecnico è che i nodi della rete siano dotati di almeno un trasmettitore e un ricevitore utilizzabili in parallelo.

Lo scenario tipico di applicazione del WBPLSec è quello delle reti wireless di sensori a basso consumo, dove questa soluzione di sicurezza può fornire dei vantaggi in termini energetici in confronto con algoritmi crittografia che operano a livello più alto [12]. Se confrontiamo WBPLSec con AES-128 possiamo subito notare alcuni vantaggi del primo rispetto al secondo quando li vogliamo usare per proteggere l'informazione scambiata tra sensori e nodi edge. AES-128 codifica le informazioni a blocchi di 128 bit, quindi il consumo di energia per la crittografia, la trasmissione e la decrittografia di un'intera stringa di bit è un multiplo dell'energia richiesta per criptare e trasmettere un blocco di 128 bit. Al contrario, l'energia richiesta da WBPLSec cresce linearmente con la lunghezza della stringa di bit evidenziando come WBPLSec risulta più efficiente da un punto di vista energetico quando devo trasmettere stringhe di bit di lunghezza inferiore ai 128 bit [12].

Un altro scenario in cui si applica WBPLSec è l'architettura edge computing (Figura 3), che mira a rispondere alla crescente domanda di calcolo a bassa latenza nelle reti IoT su vasta scala. Queste architetture includono dispositivi sensori a basso consumo energetico alimentati a

batteria che comunicano con nodi edge. I nodi edge sono connessi a un fornitore di energia e, a loro volta, comunicano con un cloud pubblico.

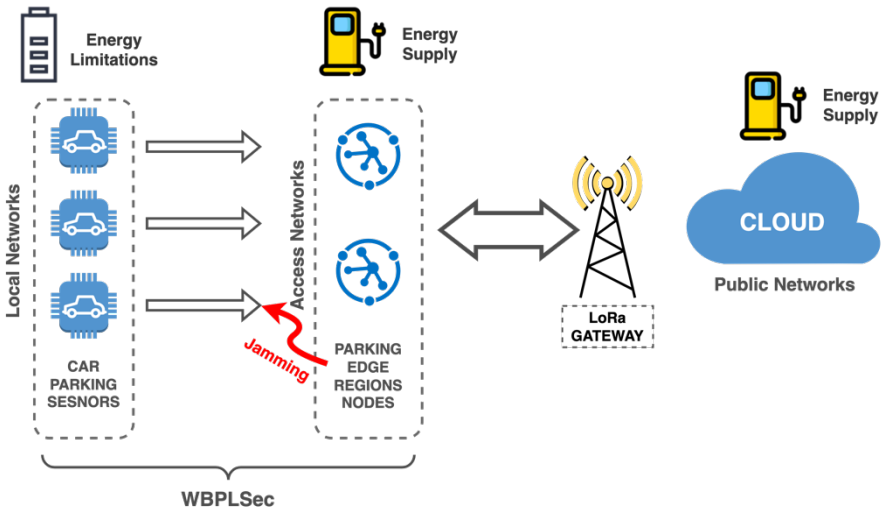

Figura 3 - Applicazione di WBPLSec in ambito reti edge [12].

In sintesi, la sicurezza basata su watermarking e jamming può essere implementata in diversi scenari applicativi, come reti wireless, architetture edge computing e applicazioni cablate, offrendo protezione a livello fisico senza richiedere eccessivo sovraccarico computazionale. Nel prossimo paragrafo ci soffermeremo su questi scenari dove è interessante applicare la sicurezza a livello fisico.

3.2 PLS nelle Comunicazioni Acustiche

Nel contesto della sicurezza delle comunicazioni a livello fisico, viene esaminata l'applicazione di un canale acustico come mezzo di comunicazione tra dispositivi elettronici. Tale canale acustico sfrutta la trasmissione di informazioni attraverso onde sonore per superare la separazione fisica tra due dispositivi che magari sono all'interno della stessa stanza ma non sono connessi direttamente tra loro; per connessioni intendiamo qualsiasi cablaggio di rete oppure qualsiasi rete wireless basata su radio frequenza.

Le emissioni acustiche dei dispositivi elettronici possono creare covert-channel, consentendo comunicazioni nascoste. Le frequenze udibili dall'orecchio umano (20 Hz - 20 kHz) e gli ultrasuoni (frequenze superiori a 20 kHz) vengono utilizzati per creare canali nascosti basati sul suono che possono bypassare i meccanismi di controllo delle informazioni. Reti nascoste basate su onde ultrasoniche sono state implementate utilizzando microfoni e altoparlanti standard per consentire comunicazioni direzionali. Dal punto di vista della sicurezza, le comunicazioni tramite ultrasuoni non richiedono autorizzazioni specifiche e possono eludere le restrizioni di sicurezza di rete. Tuttavia, ciò può essere sfruttato da un attaccante, rendendo necessarie contromisure di sicurezza adeguate. Dispositivi militari sono in grado di mitigare questo problema disabilitando il driver della scheda audio quando non in uso.
Nel 2020 è stata proposta l'applicazione del protocollo WBPLSec su un canale acustico utilizzando una gamma di frequenze ultrasoniche [14]. L'occupazione dello spettro nel canale acustico con l'applicazione del protocollo WBPLSec è mostrata nellaFigura 4.

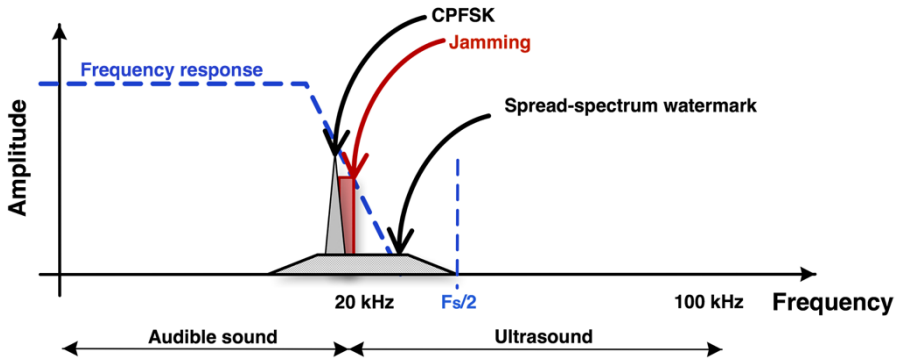

Figura 4 - Spettro di frequenze del protocollo di sicurezza a livello fisico WBPLSec nel caso delle comunicazioni acustiche [14].

È stato dimostrato con successo che WBPLSec può essere applicato a canali acustici nascosti per lo scambio di una chiave segreta condivisa di 128 bit tra mittente e destinatario che comunicano tramite altoparlanti e microfoni. Questo metodo rappresenta una tecnica preziosa per implementare la sicurezza a livello fisico, creando una regione sicura attorno al ricevitore con una distanza di fino a 2 metri.

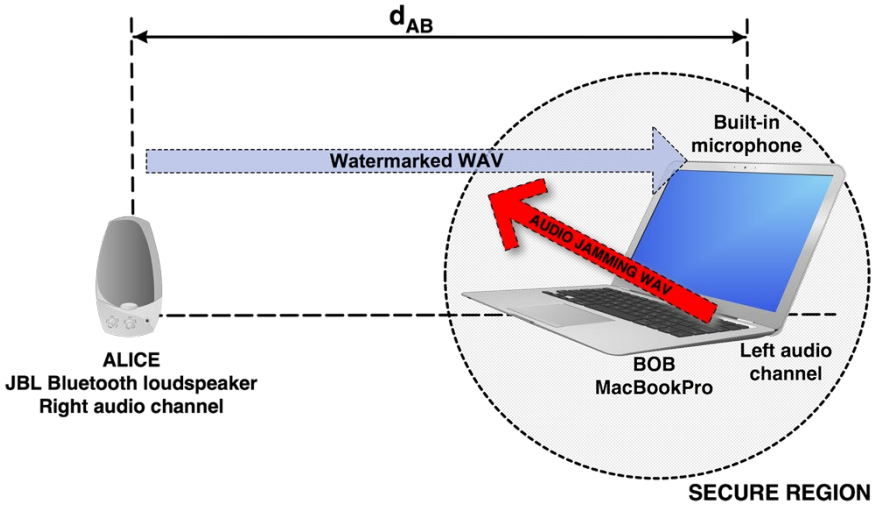

Figura 5 – Esperimenti di PLS su onde acustiche: creazione di una regione sicura attorno al ricevitore legittimo (Bob) utilizzando WBPLSec sulle comunicazioni acustiche [14].

Il protocollo WBPLSec consente a un dispositivo IoT di utilizzarlo sul canale acustico per lo scambio di una chiave segreta condivisa con un dispositivo vicino. In determinati scenari, l'utilizzo delle interfacce audio integrate nei sensori wireless esistenti può essere una soluzione conveniente, evitando la necessità di ridisegnare completamente il sensore.

Gli oggetti intelligenti wireless (IoT e Internet of Everything (IoE)) sono diffusi in vari scenari, come sistemi sanitari, case automatizzate e comunicazioni veicolari. Tuttavia, l'evoluzione dei malware richiede una revisione della sicurezza delle reti dei sensori wireless. Questo caso d'uso evidenzia l'utilizzo di un canale acustico nascosto per lo scambio sicuro di dati tra sensori wireless o come alternativa alle soluzioni tradizionali.

3.3 PLS nelle Comunicazioni Veicolari

L'aumento dell'interconnessione e dell'automazione nei sistemi automobilistici ha introdotto nuovi standard di comunicazione e connessione tra i componenti. Il Control Area Network (CAN) è ampiamente utilizzato per le reti intra-veicolari e altre applicazioni. I nodi della rete, chiamati Electronic Control Units (ECU), gestiscono diverse funzioni come il controllo del

motore, gli airbag e il sistema audio. Tuttavia, le reti CAN sono state originariamente progettate per funzionare in modo isolato, senza considerare i problemi di sicurezza o le interazioni esterne. Negli ultimi anni, con l'iperconnessione dei veicoli e l'integrazione di reti eterogenee come GPS, connessioni 4G/5G, Wi-Fi e Bluetooth, il rischio di attacchi informatici è notevolmente aumentato, poiché gli hacker possono sfruttare questa maggiore superficie di attacco.
Per garantire la sicurezza di questi sistemi e di conseguenza delle persone trasportate, è necessario progettare nuovi meccanismi di sicurezza per proteggere le comunicazioni CAN. In questo contesto numerose sono state le proposte per proteggere questi sistemi a ogni livello del modello OSI. Recentemente è stato proposto il Secure KEy DistributioN OvEr CAN (SENECAN) [13], un meccanismo innovativo che, per la prima volta in letteratura, sfrutta il jamming a livello fisico nelle comunicazioni cablate per implementare una fase sicura di distribuzione delle chiavi, con potenzialità d'uso estremamente promettenti. SENECAN implementa WBPLSec su di un bus cablato e quindi combina watermarking e jamming per garantire confidenzialità e integrità senza modificare l'architettura del protocollo.

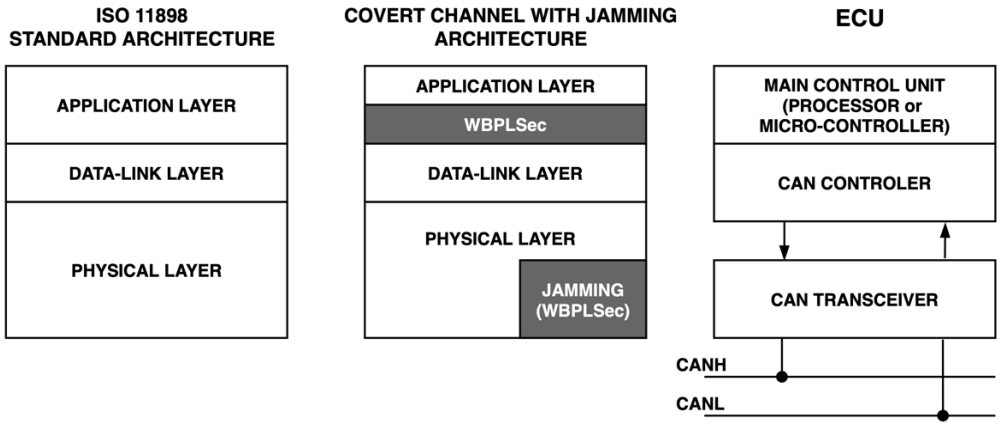

Figura 6 - Integrazione di WBPLSec nel protocollo CAN [13].

L'architettura proposta può essere considerata di tipo Bump-In-The-Stack (BITS), dove watermarking e jamming sono due funzioni atomiche che operano all'interno dello stack CAN standard (vedi Figura 6) per migliorarne la sicurezza. L'architettura dell'ECU standard non viene modificata e WBPLSec può essere implementato a livello software nel microcontrollore dell'ECU per eseguire il watermarking, mentre il trasceiver CAN viene utilizzato per eseguire il jamming sul bus.
Utilizzando questo metodo si può garantire la sicurezza delle comunicazioni. In particolare, il messaggio originale da trasmettere viene passato dal livello applicativo (cioè il microcontrollore dell'ECU) alla funzione WBPLSec, che inserisce un watermark a spettro espanso nelle informazioni prima di passarle ai livelli inferiori. Più precisamente, si utilizza il watermarking come un canale di comunicazione nascosto. Sul lato ricevente, il nodo disturba selettivamente il messaggio trasmesso sul bus CAN utilizzando la funzione di jamming aggiunta nello stack, rendendo inutilizzabile parte della comunicazione per l'attaccante.

3.4 PLS nelle Comunicazioni su onde luminose per reti 6G

L'avvento della sesta generazione (6G) delle tecnologie di comunicazione mobile rappresenta una significativa area di ricerca con un impatto rilevante sulla società. Il sistema di comunicazione di prossima generazione mira a ottenere efficienza spettrale ed energetica elevate, bassa latenza e ampia connettività, sfruttando le continue evoluzioni dei sistemi di telecomunicazione. Tuttavia, l'aumento dell'interconnessione e dell'automazione nei sistemi

automobilistici e l'utilizzo di reti IoT in scenari diversi hanno portato a una maggiore vulnerabilità agli attacchi informatici.

Le reti wireless 6G, che prevedono velocità di trasmissione dati fino a 10 Tbps, si baseranno su tecnologie abilitanti come l'intelligenza artificiale (AI), i nuovi livelli fisici, le comunicazioni semantiche, il calcolo quantistico, le reti intelligenti e le comunicazioni tramite onde luminose. Le VLC utilizzano la luce visibile per la trasmissione dei dati ad alta velocità in modo efficiente, sfruttando una banda ottica non regolata da licenze, come avviene per esempio per alcune radio, e gratuita. Questo spettro ampio e gratuito offre opportunità per comunicazioni a banda larga a basso costo, riducendo la congestione dello spettro e senza interferenze con le tecnologie wireless RF. Le VLC sfruttano l'illuminazione per la trasmissione dei dati e possono essere implementate utilizzando LED bianchi o RGB per aumentare la velocità di trasmissione.

La VLC offre caratteristiche di sicurezza intrinseche come la propagazione direzionale, la visibilità umana e il confinamento spaziale. Ad esempio, l'isolamento del segnale VLC contribuisce a migliorare la sicurezza delle comunicazioni evitando l'intercettazione all'interno di una stanza o di un edificio. Tuttavia, è necessario studiare ulteriori livelli di sicurezza per mitigare i rischi. Per esempio, WBPLSec viene applicato nelle reti VLC per migliorare la sicurezza delle comunicazioni 6G creando una regione in cui le comunicazioni tra i nodi legittimi sono protette e, al di fuori di essa, fornire informazioni sulla presenza di eventuali attaccanti.
In uno scenario del genere, si è visto che WBPLSec è in grado di mitigare attacchi come l'intercettazione, l'iniezione di messaggi, la riproduzione e la modifica dei messaggi.

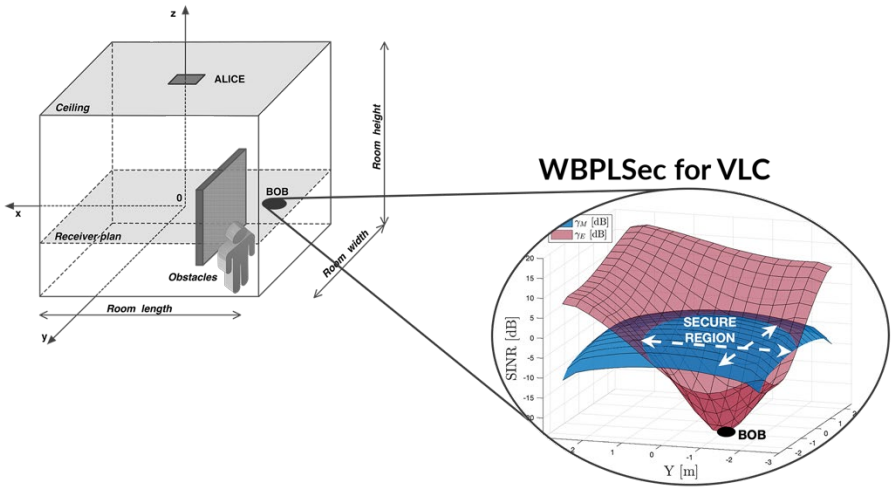

Figura 7 - Regione di sicurezza attorno al ricevitore legittimo (Bob) utilizzando WBPLSec nelle VLC [8].

In conclusione, la comunicazione VLC è considerata una tecnologia abilitante chiave per le comunicazioni wireless veloci.
Per garantire la PLS vanno affrontate diverse sfide e investigate molteplici direzioni di ricerca per il futuro sviluppo. Alcuni aspetti chiave che richiedono attenzione includono la complessità computazionale, la sicurezza contro attacchi avanzati e l'interoperabilità con altri meccanismi di sicurezza.

Complessità computazionale: La gestione delle risorse computazionali è una sfida significativa nella PLS, in quanto richiede l'elaborazione di segnali a basso livello. È fondamentale

sviluppare algoritmi e tecniche ottimizzate che garantiscano una sicurezza robusta a livello fisico con una gestione efficiente delle risorse. Ricerche future potrebbero portare all'identificazione di soluzioni che riducano la complessità computazionale senza compromettere la sicurezza.

Sicurezza contro attacchi avanzati: La PLS deve affrontare una vasta gamma di attacchi avanzati che vanno oltre le minacce tradizionali. È cruciale sviluppare meccanismi di sicurezza avanzati in grado di rilevare e mitigare tali attacchi. Le future direzioni di ricerca dovrebbero includere lo studio di tecniche di rilevamento e difesa contro attacchi di tipo man-in-the-middle, l'analisi statistica dei segnali e altre tecniche sofisticate utilizzate dagli attaccanti. L'obiettivo è garantire una protezione efficace e resiliente contro le minacce emergenti.

Interoperabilità con altri meccanismi di sicurezza: La PLS deve essere considerata come parte integrante di un sistema di sicurezza completo. È fondamentale garantire l'interoperabilità con altri meccanismi di sicurezza, come la crittografia a livello di applicazione o la sicurezza a livello di rete (p.e. livello 2 e livello 3 del modello OSI). Le ricerche future porterebbero a progettare architetture e protocolli che consentono una stretta integrazione tra la PLS e altri meccanismi di sicurezza. Questa integrazione creerebbe un ambiente sicuro in cui la PLS e gli altri meccanismi di sicurezza lavorano sinergicamente per proteggere le comunicazioni da una vasta gamma di minacce.

In conclusione, affrontare le sfide della complessità computazionale, della sicurezza avanzata e dell'interoperabilità consentirà di promuovere lo sviluppo e l'applicazione efficace della Physical Layer Security nei contesti attuali e futuri. Le ricerche in questi settori contribuiranno a rafforzare la sicurezza delle reti e delle comunicazioni, garantendo la protezione dei dati sensibili e la continuità delle operazioni.

4 Conclusioni

In un mondo sempre più interconnesso e dipendente dalle tecnologie di comunicazione, la sicurezza delle reti riveste un ruolo di fondamentale importanza. In questo contesto, la sicurezza a livello fisico (PLS) si distingue come un approccio innovativo e complementare ai tradizionali meccanismi di sicurezza. Attraverso l'utilizzo delle caratteristiche uniche dei canali di comunicazione e di altre primitive, p.e. le tecniche di watermarking e jamming, la PLS offre un'alternativa efficace per garantire la sicurezza delle comunicazioni. Nel corso di questo articolo, abbiamo esaminato diverse tecniche per la PLS e alcune sue applicazioni, evidenziando le loro peculiarità in ambiti come le comunicazioni acustiche, veicolari e su onde luminose per le reti 6G (vedi Tabella 1). Sebbene siano già stati ottenuti successi in termini di applicazione della PLS, è fondamentale continuare la ricerca per sviluppare soluzioni adatte alle reti di nuova generazione.
La PLS emerge dunque come una risorsa promettente per proteggere i dati sensibili e garantire la sicurezza nelle comunicazioni, contribuendo a preservare la continuità delle operazioni in un mondo sempre più minaccioso. L'implementazione di soluzioni di PLS rappresenta una tappa fondamentale per affrontare le sfide attuali e future nel campo della sicurezza delle reti, creando un futuro più sicuro e resiliente.

Tabella 1 - Applicazioni e tecnologie della PLS

	TECNOLOGIE			
APPLICAZIONI	**Diversità di canale**	**RIS**	**Watermarking & Jamming**	**Beamforming**
Reti di sensori wireless	✓	✓	✓	✓
Comunicazioni acustiche			✓	
Comunicazioni veicolari			✓	
Comunicazioni onde luminose – 6G	✓	✓	✓	✓

5 Riquadro 1: Valutazione della sicurezza di un sistema crittografico

Definiamo alcuni criteri utili per la valutazione della sicurezza di un sistema crittografico [15].

- **Sicurezza computazionale:** Questo criterio fa riferimento alla capacità computazionale necessaria per compromettere un sistema di crittografia. Possiamo considerare un sistema di crittografia sicuro dal punto di vista computazionale se l'algoritmo più efficiente per decifrarlo richiede almeno N operazioni, dove N è un numero estremamente grande prefissato. Purtroppo non esiste, ad oggi, alcun sistema di crittografia pratico la cui sicurezza può essere dimostrata secondo questa definizione. In campo pratico, la sicurezza computazionale di un sistema di crittografia viene spesso studiata in relazione a specifici tipi di attacchi (ad esempio, un'attacco di ricerca esaustiva della chiave). È importante notare che la sicurezza contro un particolare tipo di attacco non garantisce la sicurezza contro altri tipi di attacchi.
  Un sistema crittografico si dice computazionalmente sicuro se soddisfa almeno uno dei seguenti requisiti:
  1. Il costo della violazione del testo cifrato supera il valore delle informazioni crittografate;
  2. Il tempo richiesto per violare il testo cifrato è superiore al tempo di vita utile delle informazioni.

  L'informatica quantistica potrebbe avere un impatto enorme sulla sicurezza di molti tipi di crittografia a chiave pubblica.

- **Sicurezza dimostrabile:** Un'alternativa è fornire prove di sicurezza attraverso un processo di riduzione del problema crittografico originale. In altre parole, dimostriamo che la compromissione del sistema crittografico in esame è difficile quanto un problema che si conosce molto difficile. Questo genere di sistemi crittografici vengono talvolta etichettati come "sicuri in modo provabile", ma è fondamentale comprendere che questo metodo fornisce solo una prova di sicurezza relativa ad un altro problema, e non una prova assoluta di sicurezza.

- **Sicurezza incondizionata (o perfetta):** Questa misura riguarda la sicurezza dei sistemi crittografici quando non viene imposto alcun limite alla quantità di calcolo che un potenziale aggressore è autorizzato a eseguire. Un sistema crittografico è definito come incondizionatamente sicuro se non può essere compromesso, nemmeno con risorse computazionali illimitate.

6 Riquadro 2: Tecnologia a spettro espanso (spread spectrum (SS))

Lo spettro espanso (o spread spectrum) è una tecnica di trasmissione che diffonde un segnale di comunicazione su una banda di frequenze molto più ampia di quella strettamente necessaria per trasmettere l'informazione [12].
In pratica, lo spettro espanso viene realizzato modulando il segnale originale con una sequenza di codici pseudo-casuali, che diffonde l'energia del segnale su un'ampia banda di frequenze. Il ricevitore, conoscendo la sequenza di codici, può "ricompattare" il segnale, ricostruendo l'informazione originale.

Questo approccio ha diversi vantaggi:

1. **Riduzione delle interferenze:** Poiché il segnale è diffuso su un'ampia gamma di frequenze, è meno probabile che interferenze puntuali (come il rumore da altri dispositivi elettronici) possano interrompere l'intero segnale. Anche se parte del segnale viene disturbata, le restanti parti del segnale possono comunque trasmettere l'informazione.
2. **Sicurezza intrinseca:** Diffondere il segnale rende più difficile per i potenziali attaccanti identificare e decifrare il segnale, poiché senza conoscere l'algoritmo di diffusione specifico, il segnale appare come rumore casuale a chiunque altro tranne che al ricevitore intenzionato.
3. **Uso efficiente dello spettro:** Lo spettro espanso può consentire un uso più efficiente dello spettro radio perché diversi segnali possono sovrapporsi nello stesso spazio di frequenza senza interferire significativamente tra loro grazie a tecniche di codifica uniche. Infatti, utilizzando dei codici di espansione dello spettro tra loro ortogonali, ogni utente trasmettere e ricevere informazioni sul canale di comunicazione condiviso senza interferire con gli altri.

Questa tecnologia è alla base di molte applicazioni moderne, inclusi sistemi di comunicazione mobile, GPS e reti Wi-Fi, dove la resilienza alle interferenze e la sicurezza dei dati sono critiche.

7 Riquadro 3: Acronimi

Tabella 2 - Descrizioni degli acronimi utilizzati.

Acronimo	Significato	Descrizione
3DES	Triple Data Encryption Standard	Algoritmo di crittografia che applica tre volte il DES per aumentare la sicurezza della cifratura.
6G	Sesta Generazione	Prossima generazione delle reti mobili, con enfasi su velocità ultra-alte e latenza ultra-bassa.
AES	Advanced Encryption Standard	Standard di crittografia adottato dal governo degli Stati Uniti per proteggere le informazioni classificate.
CAN	Control Area Network	Rete di comunicazione veicolare per connettere componenti e dispositivi di controllo nel veicolo.
COST	European Cooperation in Science and Technology	Rete europea per la cooperazione e il finanziamento di ricerca e innovazione interdisciplinare.
CSI	Channel State Information	Informazioni sullo stato del canale di comunicazione utilizzate per ottimizzare la trasmissione e la ricezione.
ECC	Elliptic Curve Cryptography	Tecnologia crittografica basata sulle proprietà delle curve ellittiche, offre sicurezza con chiavi più corte.
ECU	Electronic Control Unit	Dispositivo elettronico in veicoli che gestisce una specifica funzione, come il motore o il sistema di frenata.
IoE	Internet of Everything	Estensione dell'IoT che include persone, processi e dati, oltre agli oggetti.
IoT	Internet of Things	Rete di dispositivi fisici interconnessi che raccolgono e scambiano dati.
LED	Light Emitting Diode	Diodo che emette luce quando attraversato da corrente, usato nelle VLC per trasmettere dati.
OSI	Open System Interconnection	Modello di riferimento per la standardizzazione delle comunicazioni di rete in sette livelli.
PLS	Physical Layer Security	Sicurezza implementata a livello fisico delle reti di comunicazione, sfrutta proprietà uniche dei canali.
RIS	Reconfigurable Intelligent Surface	Superfici intelligenti programmabili per manipolare onde radio o la luce e migliorare le prestazioni di comunicazione.
SNR	Signal-to-Noise Ratio	Rapporto tra il livello del segnale e il livello del rumore, indica la qualità di una trasmissione.
SS	Spread Spectrum	Tecnica di trasmissione che diffonde il segnale su una banda di frequenze più ampia del necessario.
UWB	Ultra-Wide Band	Tecnologia di comunicazione wireless che utilizza una banda molto ampia a bassa energia.
VLC	Visible Light Communication	Comunicazione tramite luce visibile, sfrutta LED per trasmettere dati.
WBPLSec	Watermarked Blind Physical Layer Security	Tecnica di sicurezza che combina watermarking e jamming per proteggere la trasmissione dei dati.

8 Biografia

Simone Soderi (SMIEEE) si è laureato nel 2002 presso l'Università di Firenze e nel 2016 ha conseguito il dottorato di ricerca (Dr. Sc. Tech) presso l'Università di Oulu in Finlandia. Le sue competenze spaziano dalla cybersecurity e dalle comunicazioni wireless all'ingegneria del software. Attualmente è assistant professor presso la Scuola IMT di Lucca e professore a contratto all'Università di Padova dove insegna "Security and risk: management and certifications" nel corso di laurea magistrale in cybersecurity. Dal 2024 è membro di gruppi di lavoro della COST Action CA22168, Physical layer security for trustworthy and resilient 6G systems (6G-PHYSEC)**.** I suoi temi di ricerca includono la cybersecurity per i sistemi di infrastrutture critiche, il 6G, i covert-channel, la sicurezza delle reti, la sicurezza del livello fisico, la sicurezza delle emissioni elettromagnetiche, le VLC e l'UWB. Il Dr. Soderi ha pubblicato articoli su riviste e conferenze oltre a capitoli di libri. È titolare di cinque brevetti sulle comunicazioni wireless e sul posizionamento veicolare.

Link istituzionale: https://sysma.imtlucca.it/people/simone-soderi

9 Bibliografia

[1] Bloch, M., Barros, J. (2011).*Physical-layer security: from information theory to security engineering*. Cambridge University Press.

[2] Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks fifth edition. In *Pearson Education, Inc.*. Prentice Hall.

[3] Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.

[4] Wyner, A. D. (1975). The wire-tap channel. *Bell system technical journal*, *54*(8), 1355-1387.

[5] Csiszár, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE transactions on information theory*, *24*(3), 339-348.

[6] Maurer, U., & Wolf, S. (2000). Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19* (pp. 351-368). Springer Berlin Heidelberg.

[7] Soderi, S., Mucchi, L., Hämäläinen, M., Piva, A., & Iinatti, J. (2017). Physical layer security based on spread-spectrum watermarking and jamming receiver. *Transactions on emerging telecommunications technologies*, *28*(7), e3142.

[8] Soderi, S., De Nicola, R. (2021). 6G networks physical layer security using RGB visible light communications. *IEEE Access*, *10*, 5482-5496.

[9] Anderson, R. (2020). *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

[10] Liu, Y., Liu, X., Mu, X., Hou, T., Xu, J., Di Renzo, M., & Al-Dhahir, N. (2021). Reconfigurable intelligent surfaces: Principles and opportunities. *IEEE communications surveys & tutorials*, *23*(3), 1546-1577.

[11] Pan, C., Ren, H., Wang, K., Kolb, J. F., Elkashlan, M., Chen, M., ... & Hanzo, L. (2021). Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions. *IEEE Communications Magazine*, *59*(6), 14-20.
[12] Proakis, J. G. (2008). *Digital communications*. McGraw-Hill, Higher Education.
[13] Costa, G., Degano, P., Galletta, L., & Soderi, S. (2023). Formally verifying security protocols built on watermarking and jamming. *Computers & Security*, *128*, 103133.
[14] Soderi, S., Colelli, R., Turrin, F., Pascucci, F., & Conti, M. (2022). SENECAN: Secure KEy DistributioN OvEr CAN Through Watermarking and Jamming. *IEEE Transactions on Dependable and Secure Computing*.
[15] Soderi, S. (2020). Acoustic-based security: A key enabling technology for wireless sensor networks. *International Journal of Wireless Information Networks*, *27*(1), 45-59.
[16] Stallings, W., Lo Re,G., & De Paola, A. (2022). *Crittografia Con MyLab*. Pearsons.
[17] Soderi, S., Brighente, A., Turrin, F., & Conti, M. (2022, September). VLC physical layer security through RIS-aided jamming receiver for 6G wireless networks. In *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 370-378). IEEE.