**TITOLO E ABSTRACT TEMA DI RICERCA DOTTORANDI DEL CORSO DI DOTTORATO DI RICERCA IN INGEGNERIA ELETTRONICA ED INFORMATICA**

# XL CICLO

## Simone Carta

**Tema di ricerca:**

*Individuazione e prevenzione dei componenti elettronici contraffatti.*

**Abstract:**

I problema della contraffazione nell'elettronica non è nuovo, ma continua a rappresentare una preoccupazione significativa ancora oggi. I componenti contraffatti possono compromettere l'affidabilità dei sistemi in cui vengono integrati e, nei casi più gravi, mettere a rischio la sicurezza delle persone e delle infrastrutture. Le dinamiche di mercato – come la carenza di componenti e l'obsolescenza – costringono spesso i clienti a rivolgersi a fonti non ufficiali, note come mercato grigio, creando condizioni favorevoli all'ingresso di prodotti contraffatti nella catena di approvvigionamento. Per ridurre il rischio che componenti elettronici contraffatti arrivino ai prodotti finali, sono fondamentali strategie sia di rilevamento che di prevenzione. In particolare, le tecniche non distruttive che possono essere integrate nei processi produttivi su larga scala sono essenziali quando ci si approvvigiona dal mercato grigio, soprattutto considerando l'evoluzione continua dei metodi di contraffazione. Questa ricerca affronta sia le tecniche non distruttive di rilevamento sia quelle di prevenzione, con un focus su soluzioni rapide e a basso costo, adatte ad applicazioni su grandi volumi di dispositivi. Per quanto riguarda il rilevamento, lo studio indaga metodi non distruttivi per identificare dispositivi con tecnologie e complessità diverse – dai semplici componenti analogici e digitali fino a sistemi complessi come le schede



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

a circuiti stampati. Per i dispositivi più semplici, si dà priorità alla caratterizzazione elettrica, mentre per i sistemi più complessi si adotterà una combinazione di caratteristiche – come l'imaging termico e le emissioni elettromagnetiche – poiché i test elettrici di base possono non risultare più sufficienti.Per quanto riguarda la prevenzione, lo studio esplora un approccio a livello di package per sviluppare un innovativo sistema di marcatura anticontraffazione basato su saggi biomolecolari. Questa strategia risulta particolarmente vantaggiosa per i prodotti già presenti sul mercato, poiché non richiede modifiche a livello di layout.

## Luigi di Michele

**Tema di ricerca:**

*Tecnologie IoT e Industria 4.0 per l'analisi e l'ingegnerizzazione di sistemi alimentari complessi nella produzione di prodotti da forno ad alto valore aggiunto nella filiera.*

**Abstract**

L'attività di ricerca è articolata in due principali ambiti. Il primo è incentrato sullo sviluppo di modelli e metodologie per la caratterizzazione dielettrica di matrici agroalimentari mediante sensori a microonde e tecniche spettroscopiche. L'obiettivo è estrarre la permittività complessa ($\varepsilon^* = \varepsilon' - j\varepsilon''$) e correlare i parametri $\varepsilon'$ ed $\varepsilon''$ con le proprietà intrinseche dei prodotti, al fine di monitorarne la qualità durante le fasi chiave del processo produttivo.Il secondo ambito riguarda il telerilevamento a microonde applicato all'agricoltura di precisione, attraverso l'utilizzo di dati radar per la stima quantitativa di variabili critiche quali l'umidità del suolo e lo stato di salute delle colture.

## Davide Ghiani

**Tema di ricerca:**

*Metodi anticontraffazione basati sull'occultamento dei dati tramite reti neurali profonde.*

**Abstract:**

Le possibilità dell'elaborazione delle immagini, del watermarking e della biometria sono cresciute, insieme ai rischi di spoofing, grazie ai progressi fatti dall'intelligenza artificiale. Il


Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

riconoscimento facciale ha assunto un ruolo centrale nei sistemi di verifica dell'identità e, per tale motivo, ICAO ha elaborato uno standard sull'acquisizione e la formattazione delle immagini di volti, oggi integrato all'interno dei "Machine Readable Travel Documents" (MRTDs) e nelle "Digital Travel Credentials" (DTCs). Tuttavia, queste immagini sono potenzialmente soggette a manipolazioni malevole, a possibili modifiche della formattazione oltre che a perdita di qualità se soggette a operazioni di stampa. Solitamente, eventuali attacchi di spoofing vengono monitorati in fase di acquisizione dai sistemi PAD (Presentation Attack Detection). Tuttavia, il bisogno di protezione persiste in caso l'immagine venga estratta, salvata o redistribuita. Lo scopo di questa ricerca consiste nello sviluppo di un metodo di autentificazione e verifica dell'integrità dell'immagine tramite l'applicazione di watermarking basati sul deep learning.

## Marco Ledda

**Tema di ricerca:**

*Apprendimento e apprendimento avversario nella progettazione e modellazione dei sistemi di controllo.*

**Abstract**

Nel campo dei sistemi e del controllo, l'integrazione delle tecniche di Machine Learning ha aperto nuove prospettive per migliorare la robustezza e le prestazioni dei sistemi. La natura complessa degli ambienti di controllo moderni implica spesso dinamiche non lineari, per le quali è difficile disporre di un modello accurato su cui poter fare affidamento. Il Machine Learning, in particolare nella forma del Deep Learning, ha dimostrato un notevole potenziale nei problemi di identificazione dei sistemi quando sono disponibili grandi quantità di dati in ingresso/uscita, consentendo così strategie avanzate di ottimizzazione e controllo. Tuttavia, una questione fondamentale riguarda lo sviluppo di garanzie formali sull'affidabilità e la robustezza di questi metodi. Questa proposta di ricerca si propone di esplorare la sinergia tra sistemi di controllo e machine learning per sviluppare tecniche robuste di identificazione e controllo dei sistemi, e testare la robustezza di tali sistemi con un focus anche sulla progettazione di strategie di difesa contro attacchi di apprendimento avversario.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

L'integrazione tra machine learning e sistemi di controllo nasce dalla necessità di superare i limiti dei metodi di controllo tradizionali quando si ha a che fare con sistemi dinamici complessi e non lineari. Le strategie di controllo tradizionali sono oggi considerate più robuste, poiché offrono garanzie formali in termini di stabilità. Tuttavia, in assenza di modelli formali accurati, il machine learning può contribuire a migliorare la progettazione del controllo. Inoltre, la comunità scientifica sta conducendo numerosi studi per fornire garanzie formali anche ai metodi di controllo basati su tecniche di machine learning, in termini di stabilità e robustezza. L'obiettivo generale della ricerca è sviluppare un framework integrato che combini il Machine Learning con la progettazione dei sistemi di controllo e sfrutti tecniche di apprendimento avversario per identificare modalità di guasto e vulnerabilità rispetto ad attacchi informatici e fisici (cyber-fisici).

## Federico Manca

**Tema di ricerca:**

*Metodologie di calcolo approssimato a livelli misti in coprocessori hardware riconfigurabili.*

**Abstract**

La ricerca si concentra sull'applicazione di metodologie di calcolo approssimato su coprocessori hardware riconfigurabili, più precisamente sugli acceleratori di reti neurali basati su FPGA. L'obiettivo è sviluppare soluzioni efficienti per l'implementazione di modelli complessi di deep learning su dispositivi edge, che spesso devono rispettare vincoli rigorosi in termini di utilizzo delle risorse, consumo energetico, area occupata e latenza. Attraverso tecniche come la quantizzazione, l'ottimizzazione dell'architettura e la precisione a livelli misti, questo lavoro mira a ridurre il costo computazionale mantenendo prestazioni accettabili, facilitando così l'integrazione dell'intelligenza artificiale in scenari embedded.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

## Emmanuele Massida

**Tema di ricerca:**

*Tecniche di rilevamento e mitigazione delle vulnerabilità: sviluppo di soluzioni con protezione della privacy nelle tecnologie emergenti.*

**Abstract:**

L'obiettivo di questo progetto di ricerca è investigare e sviluppare tecniche di rilevamento e mitigazione delle vulnerabilità, con un particolare focus su approcci attenti alla privacy, adatti a tecnologie emergenti come WebAssembly. Il progetto affronta le crescenti sfide di cybersecurity associate all'adozione di nuove tecnologie digitali, in particolare le vulnerabilità derivanti dalla compilazione di linguaggi di programmazione tradizionali in WebAssembly e le intrusioni alla privacy insite negli strumenti di sicurezza contemporanei. La ricerca mira ad analizzare in modo approfondito le vulnerabilità introdotte dalle tecnologie emergenti, sviluppare e perfezionare soluzioni di sicurezza non invasive e orientate alla protezione della privacy, e migliorare gli strumenti esistenti di reverse engineering e rilevamento malware.Le metodologie adottate combinano analisi statica e dinamica, machine learning, deep learning e l'uso di modelli linguistici di grandi dimensioni per esplorare nuove minacce informatiche e strategie di mitigazione. I risultati attesi includono una valutazione esaustiva delle vulnerabilità dimostrata attraverso Proof of Concept, strumenti innovativi di reverse engineering progettati per migliorare la sicurezza, tecniche anti-malware privacy-aware con relativi dimostratori, e soluzioni di sicurezza adattabili efficaci in diversi ambienti, inclusi desktop, mobile e piattaforme cloud. In ultima analisi, il progetto si propone di ampliare significativamente lo stato dell'arte della cybersecurity, promuovendo una maggiore consapevolezza e migliori pratiche di sicurezza e privacy all'interno dell'ecosistema digitale.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

## Luca Minnei

**Tema di ricerca:**

*Android Malware Operation*

**Abstract:**

La ricerca si concentra sull'affrontare la minaccia significativa rappresentata dai malware Android, resa particolarmente complessa dalla rapida comparsa di nuove varianti. Gli attuali classificatori statici diventano spesso obsoleti, lasciando molti dispositivi vulnerabili, poiché non esiste una soluzione che aggiorni automaticamente i modelli di rilevamento per stare al passo con l'evoluzione delle minacce. Per affrontare questo problema, questa ricerca di dottorato si focalizzerà sulla creazione di una nuova pipeline auto-aggiornante, in grado di garantire che i rilevatori di malware Android mantengano la loro efficacia nel tempo. Il sistema sarà progettato per raccogliere nuove applicazioni e informazioni sulle minacce da fonti affidabili, come AndroZoo e VirusTotal, con cadenza trimestrale. I dati raccolti saranno aggiunti a un ampio dataset per l'analisi. Attraverso l'impiego di tecniche di apprendimento continuo (continual learning), la pipeline riaddestrerà un insieme di rilevatori statici, consentendo loro di integrare nuove varianti di malware senza dimenticare quelle precedenti. Inoltre, verranno implementate strategie di active learning per dare priorità all'annotazione manuale dei campioni più informativi. Una volta aggiornati, i modelli saranno salvati insieme a report sulle prestazioni, rendendoli immediatamente disponibili per l'implementazione. Automatizzando i processi di raccolta dati, riaddestramento e rilascio dei modelli, questo framework si propone di offrire una difesa costantemente aggiornata contro i malware, riducendo al minimo l'intervento manuale.

## Marco Murgia

**Tema di ricerca:**

*Modellizzazione avanzata della propagazione in ambienti urbani complessi per le reti cellulari 5G e applicazione di tecnologie a radiofrequenza non distruttive.*

**Abstract**



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

L'attività di ricerca si articola in due direzioni principali. La prima si concentra sul miglioramento dei modelli empirici di propagazione radio, come il COST 231 Walfisch-Ikegami e l'ITU R P.1411, con l'obiettivo di perfezionare la previsione della copertura 5G in ambienti urbani complessi. Lo studio prevede il confronto tra diversi modelli (deterministici, empirici e basati sul machine learning), integrati con simulazioni e misure sperimentali, al fine di sviluppare un modello predittivo più accurato a supporto della progettazione della rete 5G. La seconda linea di ricerca è dedicata all'uso della spettroscopia a microonde per il rilevamento rapido e non invasivo dell'adulterazione.

## Jefferson David Rodriguez Chivata

**Tema di ricerca:**

*Metodi di steganografia e watermarking per il rilevamento proattivo di DeepFake nelle immagini facciali.*

**Abstract**

Negli ultimi anni, la tecnologia DeepFake è cresciuta rapidamente, rendendo possibile la creazione di immagini e video falsi molto realistici, soprattutto dei volti. Ciò solleva serie preoccupazioni per la privacy, la fiducia e la diffusione di informazioni false. I metodi tradizionali per rilevare i DeepFake spesso reagiscono dopo che il contenuto falso è già stato creato e potrebbero non funzionare bene contro le nuove e più avanzate tecniche di DeepFake. Questo progetto di ricerca si concentra sull'utilizzo della steganografia e del watermarking come strumenti proattivi per aiutare a fermare i DeepFake prima che si diffondano. Queste tecniche funzionano nascondendo informazioni invisibili all'interno delle immagini facciali prima di essere incorporate nel web o in applicazioni specifiche. In seguito, se qualcuno modifica o manipola l'immagine utilizzando strumenti DeepFake, le informazioni nascoste possono aiutare a rilevare le modifiche e a dimostrare se l'immagine è reale o falsa. L'obiettivo è progettare modi intelligenti per aggiungere queste informazioni nascoste in modo che rimangano forti anche dopo che l'immagine è stata modificata o condivisa online. Allo stesso tempo, non deve influire sull'aspetto dell'immagine. In questo modo, intendiamo migliorare il rilevamento dei DeepFake, proteggere l'identità delle persone e rendere i



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

contenuti digitali più affidabili. Questo lavoro può supportare aree importanti come la sicurezza digitale, la verifica delle notizie e le indagini penali. Contribuirà a costruire un mondo online più sicuro e affidabile, in cui le persone possano fidarsi delle immagini che vedono.

## XXIX CICLO

### Simone Carta

**Tema di ricerca:**

*Rilevamento di falsificazioni per il potenziamento di sistemi di riconoscimento dell'impronta digitale e dell'iride.*

**Abstract**

Con la crescente diffusione di sistemi biometrici per l'autenticazione e l'identificazione personale, la sicurezza contro attacchi di falsificazione (spoofing) è diventata una sfida prioritaria. In particolare, le modalità biometriche basate sull'impronta digitale e sull'iride, pur offrendo elevati livelli di accuratezza, risultano vulnerabili a tecniche di presentazione artefatte, come l'uso di dita in silicone, immagini ad alta risoluzione o contatti a stampa dell'iride. Il presente lavoro propone un approccio avanzato per il rilevamento automatico di falsificazioni, finalizzato a potenziare l'affidabilità e la resilienza dei sistemi biometrici unimodali e multimodali. La metodologia adottata non si basa più sull'estrazione manuale di caratteristiche tessiturali della biometria, bensì su moderne tecniche di visione artificiale e deep learning che negli anni più recenti hanno dimostrato la propria efficacia in diversi campi applicativi del riconoscimento di pattern in immagini, con particolare attenzione all'utilizzo di reti neurali convoluzionali (CNN) addestrate su dataset realistici contenenti sia campioni autentici che tentativi di attacco.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

## Giuseppe Floris

**Tema di ricerca:**

*Intelligenza Artificiale Robusta per Applicazioni di Sicurezza Informatica.*

**Abstract:**

Le applicazioni web sono esposte a minacce in continua evoluzione e sempre più complesse, come SQL injection (SQLi), cross site scripting (XSS), server side request forgery (SSRF) e violazioni della privacy, che sfuggono facilmente ai tradizionali sistemi basati su firme o regole. Per questo motivo si è fatto largo l'impiego di soluzioni basate sull'intelligenza artificiale, sistemi in grado di apprendere nuovi schemi di attacco e individuare vulnerabilità in tempo reale, bloccando exploit che le tecniche convenzionali non riescono a intercettare. Tuttavia, l'uso diffuso dell'IA in contesti altamente critici solleva questioni di affidabilità, robustezza, protezione della privacy e rischi potenziali. Queste minacce hanno il potenziale per diventare più sofisticate nel tempo per eludere i modelli addestrati su schemi già noti. Di conseguenza, è necessario un continuo retraining su dati aggiornati, ma ciò introduce il rischio di regressione, compromettendo le prestazioni del modello nel rilevare gli exploit già noti. Inoltre, i sistemi di intelligenza artificiale per la sicurezza delle applicazioni web sono anche vulnerabili agli esempi avversari in cui un aggressore modifica impercettibilmente l'input per causare una classificazione errata del modello, rendendo essenziali le misure di robustezza per prevenire potenziali exploit. Questa ricerca si concentra sullo sviluppo di modelli di apprendimento automatico robusti e affidabili, in grado di mantenere prestazioni elevate anche in presenza di dati manipolati o condizioni inaspettate, nel settore della sicurezza informatica. In particolare, la ricerca esplora tecniche di difesa, come l'adversarial training (addestramento su esempi avversari), il rilevamento di tentativi di evasione e l'adozione di strategie di progettazione orientate alla robustezza dei modelli, e studia l'integrazione di tali modelli robusti in applicazioni pratiche per la sicurezza di sistemi e reti. Inoltre, una parte fondamentale del lavoro è la valutazione sistematica della robustezza utilizzando attacchi avversari, ossia la generazione di input avversari che consentono l'identificazione delle vulnerabilità residue e il miglioramento iterativo delle difese proposte. L'obiettivo principale è quello di garantire la resilienza dei sistemi di AI di sicurezza alle



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

interruzioni dolose, migliorando al contempo la loro capacità di generalizzazione a nuovi tipi di attacco. Questo obiettivo viene raggiunto analizzando l'intera pipeline, dalle caratteristiche dei dati di input all'architettura del modello fino alle metriche di valutazione, al fine di comprendere le loro interazioni e il loro impatto sulle prestazioni complessive. Considerando la continua evoluzione degli attacchi alle applicazioni web, la regressione delle prestazioni e la robustezza contro gli attacchi avversari, la ricerca mette in evidenza la complessità delle pipeline nella cybersecurity e mira a contribuire allo sviluppo di sistemi di cybersecurity che garantiscano affidabilità, resilienza e siano in grado di far fronte ad attacchi sempre più sofisticati nel tempo.

## Marco Garau

**Tema di ricerca:**

*Un'analisi "What-If" guidata dai dati per favorire il passaggio dall'auto privata ai servizi di trasporto pubblico.*

**Abstract**

La crescita urbana e la crescente domanda di mobilità stanno mettendo a dura prova la pianificazione dei trasporti, che richiede dati sempre più accurati sui modelli di mobilità per proporre soluzioni efficaci. Questa ricerca contribuisce ad affrontare questa sfida proponendo un modello e un'implementazione pratica dell'analisi "What-If" per supportare la progettazione di sistemi MaaS (Mobility as a Service) integrando dati sulla domanda di mobilità provenienti dal crowdsourcing e dati sul trasporto pubblico attraverso GTFS (General Transit Feed Specification). Concentrandoci sulla città di Cagliari, utilizziamo i dati ottenuti dal progetto di crowdsoucing "IoPollicino" per analizzare i modelli di mobilità e validare il nostro modello. Lo studio introduce diverse metriche, combinando fattori spaziali e temporali per confrontare i servizi di trasporto pubblico (PT) con gli spostamenti privati e per identificare i percorsi chiave del PT da migliorare. Il modello simula scenari alternativi per ottimizzare il trasporto pubblico, gettando le basi per una mobilità urbana sostenibile utilizzando le tecnologie di analisi dei big data. I risultati rivelano le carenze del trasporto pubblico in termini di copertura spaziale e tempistica, dimostrando che molti spostamenti



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

privati potrebbero passare al trasporto pubblico, garantendo una migliore accessibilità e frequenza.

## Usama Mahmood

**Tema di ricerca:**

*Sviluppo di sistemi elettronici flessibili per applicazioni nell'ambito della soft robotics.*

**Abstract**

L'attività di ricerca del dottorando Usama Mahmood si esplica principalmente all'interno del Progetto Europeo BIOMELD, e riguarda lo sviluppo di sistemi elettronici flessibili per il controllo e il monitoraggio in tempo reale di particolari *soft robots* dette "macchine bioibride". Tali sistemi sono realizzati su substrati plastici ultra-flessibili, di spessore non superiore ai 2 micrometri, e comprendono sia sensori per il monitoraggio del movimento del robot, come ad esempio sensori di strain, sia elettrodi per l'attuazione di tessuti cellulari integrati nel robot e responsabili del suo movimento. La tecnologia utilizzata è quella dell'elettronica organica, coinvolgendo principalmente processi tecnologici a basso costo ed elevata area di lavoro come la stampa a getto di inchiostro.

## Luca Martis

**Tema di ricercar:**

*Lightweight Spiking Neural Networks for Edge Computing.*

**Abstract:**

Il settore dell'Edge AI per i dispositivi indossabili a bassissimo consumo è una frontiera in rapida evoluzione con un significativo potenziale di trasformazione. In questo contesto, le reti neurali Spiking (SNN) hanno attirato una crescente attenzione grazie al loro modello di calcolo efficiente dal punto di vista energetico e guidato dagli eventi, che le rende particolarmente adatte ad applicazioni con risorse limitate. Queste reti raggiungono le migliori prestazioni su processori neuromorfi dedicati, progettati specificamente per sfruttare la scarsità di eventi e massimizzare l'efficienza computazionale. Attualmente, diversi



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

processori neuromorfici specializzati si sono dimostrati molto efficaci nell'esecuzione di SNN su larga scala, mantenendo un'efficienza energetica impressionante. Tuttavia, nonostante le promesse, l'adozione diffusa dell'hardware neuromorfico rimane limitata dagli alti costi di sviluppo e dalla limitata accessibilità. L'obiettivo di questo progetto è lo sviluppo di sistemi hardware personalizzati per l'esecuzione efficiente di algoritmi basati su reti neurali Spiking, offrendo un'alternativa agli acceleratori neurali attualmente disponibili. L'obiettivo è superare le barriere poste dagli alti costi di sviluppo e dalla limitata accessibilità delle soluzioni neuromorfiche esistenti, con particolare attenzione all'integrazione in dispositivi edge a bassissimo consumo.

## Raffaele Mura

**Tema di ricerca:**

*Intelligenza Artificiale interpretabile e sicura.*

**Abstract:**

I recenti progressi nell'ambito della generative artificial intelligence, tra cui i large language models (LLMs), la retrieval-augmented generation (RAG) e le architetture multimodali, hanno reso possibili sistemi capaci di elaborare input diversi, come immagini e testi, per svolgere compiti complessi come la conversazione, il ragionamento e il recupero di contenuti. Sebbene questi modelli mostrino capacità notevoli, introducono allo stesso tempo nuovi rischi in termini di sicurezza e affidabilità, molti dei quali risultano ancora poco esplorati. Il progetto di ricerca affronta queste criticità, analizzando come manipolazioni dell'input sottili e strategicamente progettate possano compromettere il comportamento dei modelli ed eludere le difese esistenti. Lo studio analizza scenari di attacco come le prompt injection ottimizzate, che mirano a indurre i modelli a generare risposte dannose o inappropriate, e gli attacchi di data poisoning, che corrompono le knowledge base dei sistemi di retrieval. Una parte fondamentale di questo lavoro consiste nell'analizzare le rappresentazioni interne dei modelli, con un'attenzione particolare alle feature latenti e agli embedding spaces. Questo tipo di analisi mira a interpretare i meccanismi di ragionamento interno del modello, a comprendere come il modello apprende i dati di training e come



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

vengono prese le decisioni, oltre a esplorare in che modo avversari potrebbero sfruttare queste caratteristiche interne o come potrebbero essere utilizzate per rafforzare la robustezza dei modelli. Attraverso l'analisi di questi scenari di attacco, il progetto intende mettere in luce i limiti degli attuali meccanismi di sicurezza e dimostrare quanto sia facile sovvertire il comportamento dei modelli, spesso senza essere rilevati. Un'analisi approfondita di queste vulnerabilità contribuirà a una comprensione più chiara delle minacce avversarie nell'ambito della generative AI. L'obiettivo finale è fornire linee guida concrete per sviluppare sistemi di machine learning più sicuri, robusti e affidabili, capaci di resistere agli attacchi avversari in applicazioni pratiche e reali.

## Andrea Panzino

**Tema di ricerca:**

*Metodi e modelli di rilevamento di artefatti facciali basati su "morphing" e "deepfake" per la trasmissione sicura di foto per documenti d'identità.*

**Abstract:**

Negli ultimi anni, l'integrazione di tecniche avanzate di manipolazione visiva con modelli di deep learning di ultima generazione ha evidenziato criticità rilevanti in ambito cybersecurity, in particolare rispetto alla resilienza dei sistemi di autenticazione biometrica. Una delle vulnerabilità più insidiose emerse è rappresentata dal face morphing, una tecnica atta a generare immagini facciali sintetiche mediante la fusione tra due (o più) volti reali. Un'ulteriore minaccia rilevante in questo ambito è rappresentata dai deepfake, ovvero contenuti multimediali sintetici generati tramite tecnologie avanzate di intelligenza artificiale, quali Generative Adversarial Networks (GANs) o modelli di trasformazione neurale. Tali tecniche consentono la produzione di video, immagini e audio contraffatti con un elevato grado di realismo, al punto da compromettere l'affidabilità dei sistemi di sicurezza nel distinguere tra dati autentici e manipolazioni digitali. Il presente lavoro di ricerca si propone di analizzare in profondità queste tecniche di attacco e di progettare metodologie innovative per la loro rilevazione automatica, attraverso lo sviluppo di detector robusti e



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

facilmente integrabili all'interno delle architetture di autenticazione biometrica attualmente in uso.

## Diego Soi

**Tema di ricerca:**

*Analisi dei Malware Android: uno studio su tecniche di analisi, rilevamento e offuscamento.*

**Abstract:**

Al giorno d'oggi, i dispositivi mobili sono ampiamente utilizzati nelle attività quotidiane, non limitandosi più alle operazioni di base come messaggi e chiamate, ma includendo anche compiti legati alla sicurezza, come l'Autenticazione a Più Fattori (MFA), lo sblocco di un'auto, di una cassetta di sicurezza o l'accesso al mobile banking. Di conseguenza, il software malevolo rappresenta una minaccia significativa per la sicurezza e la privacy degli utenti. Queste minacce vengono mitigate da sistemi anti-malware, spesso basati su tecniche di Machine Learning e Deep Learning. Tuttavia, una sfida cruciale che la ricerca deve affrontare è l'aumentata variabilità, in termini di comportamento, dei campioni malevoli. Pertanto, questo progetto si propone di esplorare nuove tecniche per analizzare e rappresentare le applicazioni Android in modo adeguato per i sistemi basati su Intelligenza Artificiale. In particolare, l'attenzione è rivolta a due componenti fondamentali: l'interpretabilità degli algoritmi, per spiegare il processo di ragionamento dei modelli sottostanti; e la robustezza dei rilevatori contro attacchi basati su tecniche di offuscamento tradizionali, ad esempio la rinomina delle classi e l'iniezione di codice morto, e su tecniche innovative, come la steganografia per nascondere il payload malevolo.

## **Bohan Cui** (co-tutorship with Xidian University, Xi'an, China.)

**Tema di ricerca:**

*Analisi teorica dei giochi e sintesi dei sistemi cyber-fisici.*

**Abstract**



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Con i sistemi sempre più connessi in rete e aperti, i dati di percezione e decisione sono spesso attaccati o manomessi da intrusi esterni, il che minaccia le prestazioni e la sicurezza dei sistemi. Pertanto, oltre al “sistema” e all'“ambiente”, che sono oggetto della tradizionale teoria del controllo di supervisione dei sistemi, l'“avversario”, come nuovo elemento, sta emergendo sempre più nel problema dell'analisi e della sintesi in un ambiente interattivo aperto. Ciò comporta nuove sfide per la ricerca sull'analisi dei sistemi e la sintesi dei controllori. Pertanto, ci proponiamo di introdurre l'idea della teoria dei giochi nei sistemi a eventi discreti, di rappresentare l'interazione tra il sistema e l'avversario in un ambiente interattivo aperto e di sintetizzare un supervisore sicuro per questo tipo di sistemi. Questo problema viene definito teoria del controllo di supervisione sotto attacco, che ha attirato molta attenzione negli ultimi anni. Tuttavia, l'idea di base dei lavori citati si basa sull'ipotesi che il modello di azione dell'avversario sia noto in anticipo. Questo modello limita il fatto che l'avversario non possa adattare il proprio comportamento in base a quello del supervisore. A tal fine, è necessario introdurre l'idea della teoria dei giochi nell'analisi dei sistemi a eventi discreti e nella teoria del controllo di supervisione.

## XXXVIII CICLO

### Lorenzo Agostino Cadinu

**Tema di ricerca:**

*Sviluppo di un Dispositivo Basato sulla Fluorescenza e di un Algoritmo Predittivo per il Monitoraggio della FMN nella Perfusione Meccanica di Organi Umani.*

**Abstract**

Le liste di attesa per un trapianto d’organo sono in costante crescita a livello globale, con un numero significativo di pazienti che diventano non idonei al trapianto o muoiono prima di ricevere un organo. Negli ultimi anni, la machine perfusion si è affermata come una tecnica innovativa per la preservazione degli organi, permettendo anche una valutazione funzionale pre-trapianto. In questo contesto, la Flavina Mononucleotide (FMN) è emersa come un biomarcatore promettente: il suo rilascio dai mitocondri, causato dal danno da



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

ischemiariperfusione, è fortemente correlato agli esiti post-trapianto. La sfida principale risiede nella rilevazione efficace e in tempo reale di FMN nel liquido di perfusione. Questo progetto di dottorato ha sviluppato un dispositivo innovativo basato sulla fluorescenza, capace di rilevare e quantificare l'FMN durante la perfusione di diversi organi umani (cuore, polmone, fegato, pancreas, intestino). L'integrazione di un algoritmo avanzato consente non solo la quantificazione accurata, ma anche la predizione dei livelli futuri di FMN e dell'esito posttrapianto, prima ancora che l'intervento venga effettuato. I test clinici hanno confermato l'affidabilità e le elevate prestazioni del sistema. Questo lavoro rappresenta un passo significativo verso una medicina dei trapianti più predittiva, personalizzata ed efficiente.

## Elena Ferrazzano

**Tema di ricerca:**

*Sensorizzazione di arto protesico.*

**Abstract**

L'obiettivo principale delle protesi di arto superiore è quello di creare un dispositivo in grado di imitare la sua controparte umana in tutti gli aspetti sia estetici sia funzionali. Alcuni aspetti risultano essenziali per la sensazione di appartenenza dell'arto protesico e di conseguenza per l'accettazione o il rifiuto dello stesso, uno tra questi è la sensorizzazione dell'arto. Tramite l'utilizzo di sensori è infatti possibile creare una protesi in grado di eseguire prese forti con più dita, manipolazioni fini e precise con un solo dito, nonché la ricreazione della percezione degli oggetti e dunque di un feedback sensoriale. L'obbiettivo della sensorizzazione è quello di fornire informazioni sufficienti per il controllo della protesi e di tutte le fasi del processo di presa, vale a dire avvicinamento all'oggetto, il contatto con esso, sollevamento/utilizzo, posizionamento e fine del contatto, oltre a consentire un feedback tattile all'utente. Il presente progetto di ricerca, in collaborazione con Prensilia SrL., si inserisce all'interno del progetto MAGNELIQ finanziato dal programma di ricerca e innovazione Horizon 2020 dell'Unione Europea e con l'obiettivo di sviluppare un nuovo materiale liquido magnetoelettrico (ME) e creare sensori a forza distribuita per robotica e



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

protesi che sfruttano le caratteristiche uniche di tale materiale. Un materiale ME è caratterizzato da proprietà magnetiche che possono essere manipolate con un campo elettrico e viceversa. I vantaggi di utilizzare un liquido all'interno di un sensore sono molteplici tra i quali la flessibilità rispetto ai solidi e dunque la possibilità di essere realizzati di qualsiasi forma e dimensione. Ad oggi non esistono molti sensori di forza che integrano dei liquidi al loro interno e la maggior parte di questi il liquido viene posto in prossimità del polpastrello rendendoli fragili; infatti, un eventuale danneggiamento porterebbe alla fuoriuscita del liquido stesso. Con il presente lavoro si vuole realizzare un sensore di forza che possa essere inserito all'interno della protesi. Il sensore comprendente un componente di rilevamento e un componente deformabile formato da un elastomero magnetico. Il componente deformabile cambia forma sotto un carico esterno che viene percepito dalla componente sensibile attraverso l'interazione magnetica. L'elastomero agisce come un magnete distribuito posto sopra il componente sensibile. Il componente sensibile comprende una camera che racchiude il liquido ME e una matrice di elettrodi.

## Mohammadali Hamidi

**Tema di ricerca:**

*Enhancing User Quality of Experience in Multimedia Environments: Subjective and Objective Approaches for Image and Point Cloud Content.*

**Abstract**

Nel panorama in rapida evoluzione dei media immersivi e delle tecnologie di comunicazione, garantire un'elevata qualità dell'esperienza (QoE) per gli utenti finali è diventata una sfida centrale. Questa ricerca mira a far progredire la comprensione e la modellazione della QoE nelle reti multimediali, con particolare attenzione ai contenuti visivi complessi come le immagini 2D e i dati 3D a nuvola di punti. Il lavoro integra studi soggettivi sugli utenti con lo sviluppo di modelli di previsione oggettivi per valutare e migliorare la QoE in una varietà di formati multimediali e condizioni di rete. Gli esperimenti soggettivi sono progettati per catturare le valutazioni percettive degli utenti in condizioni controllate, fornendo una verità di base affidabile per la valutazione della qualità. I set di dati comprendono sia immagini



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

naturali che viste proiettate di nuvole di punti dinamiche/statiche, elaborate con vari tipi e livelli di distorsione. Dal punto di vista oggettivo, vengono impiegati modelli di apprendimento automatico e di deep learning per prevedere la qualità percepita dagli utenti a partire da caratteristiche visive e di rete. Questi modelli sfruttano le intuizioni dei dati soggettivi raccolti e incorporano caratteristiche sia artigianali che derivate dai dati per migliorare l'accuratezza della previsione e la generalizzazione. In definitiva, questa ricerca contribuisce alla progettazione di sistemi multimediali più incentrati sull'utente, fornendo strumenti e approfondimenti per la misurazione e l'ottimizzazione della QoE sia nei contenuti di immagini tradizionali sia nei formati volumetrici emergenti, come i cloud point.

## Nasreddine Makni

**Tema di ricerca:**

*Sviluppo di sensori innovativi per il rilevamento diretto dello stato idrico delle piante al fine di ottimizzare la gestione dell'irrigazione.*

**Abstract**

Il settore agricolo, in particolare nei Paesi dell'area mediterranea, si trova ad affrontare crescenti problematiche legate alla scarsità d'acqua, aggravate dagli effetti sempre più evidenti dei cambiamenti climatici. In questo contesto, l'agricoltura di precisione si è affermata come una delle strategie più promettenti per migliorare l'efficienza nella gestione delle risorse idriche e aumentare la produttività delle colture. Tuttavia, gli strumenti di monitoraggio tradizionali come i sensori di umidità del suolo e le stazioni meteorologiche offrono solo una valutazione indiretta delle esigenze idriche delle piante, risultando spesso insufficienti per garantire un'irrigazione realmente mirata ed efficiente. La presente ricerca di dottorato si propone di sviluppare biosensori innovativi e non invasivi, in grado di rilevare direttamente lo stato idrico della pianta. Questi dispositivi permetteranno di ottenere dati in tempo reale e altamente precisi su quanto e quando irrigare, migliorando in modo significativo la gestione dell'irrigazione. L'obiettivo finale è duplice: da un lato, ridurre al minimo gli sprechi d'acqua; dall'altro, promuovere pratiche agricole più sostenibili e resilienti. I sensori proposti rappresentano un progresso concreto nel campo dell'agricoltura



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

di precisione, offrendo soluzioni scalabili ed efficaci per affrontare le sfide ambientali attuali e future.

## Gianpaolo Perrelli

**Tema di ricerca**

*Verifica dell'autenticità dell'identificazione automatica per mezzo di biometrie fisiologiche e comportamentali, analisi di contesto e relative tecniche di gestione dei dati.*

**Abstract**

L'autenticità delle informazioni è diventata una sfida critica negli ultimi anni. Ogni giorno affidiamo a sistemi digitali il compito di autenticarci e connetterci con il mondo, ma l'avvento di tecniche per generare contenuti sintetici iperrealistici minaccia questa fiducia. Viviamo in un'era in cui ogni dato è un potenziale falso, per proteggere l'integrità dei sistemi, è essenziale sviluppare tecnologie avanzate in grado di distinguere il reale dal manipolato, soprattutto in applicazioni che gestiscono dati sensibili. Nonostante i progressi nella rilevazione dei deepfake, molte soluzioni trascurano uno scenario cruciale: i video sottoposti a trasformazioni semplici ma diffuse, come le compressioni automatiche applicate dai social network. Questi algoritmi, infatti, eliminano proprio quelle informazioni che i detector sfruttano per identificare i falsi, rendendoli inefficaci in contesti reali. Questa ricerca affronta il problema su due fronti: sviluppo di metodi avanzati per contrastare i deepfake anche in condizioni critiche; implementazione di approcci non invasivi per prevenire accessi illeciti ai dispositivi, sfruttando esclusivamente i sensori integrati negli smartphone per riconoscere l'utente autorizzato in modo automatico e trasparente.

## Giovanni Pettorru

**Tema di ricerca**

*Servizi di localizzazione di nuova generazione: Soluzioni di posizionamento senza GPS per ambienti IoT.*

**Abstract**



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

Negli ultimi anni, la comunità scientifica si è concentrata sulle sfide della localizzazione, dell'assegnazione dei compiti e dell'orchestrazione della rete all'interno di ambienti IoT complessi. In questa direzione, i servizi basati sulla localizzazione (LBS) svolgeranno un ruolo cruciale nel consentire soluzioni intelligenti e consapevoli del contesto che si adattano all'ambiente operativo. Tuttavia, la dipendenza da sistemi di posizionamento basati su satelliti come il GPS limita l'efficacia di questi servizi, soprattutto in aree interne o ostruite con scarsa copertura. Questa ricerca affronta queste sfide sviluppando tecniche di localizzazione prive di GPS basate su misurazioni dell'intensità del segnale ricevuto (RSS), che offrono stime affidabili della posizione dei dispositivi in ambienti reali senza richiedere infrastrutture complesse. Un aspetto fondamentale di questo lavoro è l'uso di approcci ibridi che integrano dati provenienti da più tecnologie con considerazioni statistiche ed euristiche, garantendo la robustezza contro le interferenze ambientali e gli attacchi alla rete, come la manipolazione del segnale. Questo approccio migliora sia l'affidabilità del posizionamento che la sicurezza del processo decisionale basato sulla posizione. Le soluzioni proposte sono state convalidate in scenari reali, con particolare attenzione al settore della Smart Agriculture. In queste applicazioni, i dispositivi IoT commerciali sono utilizzati per monitorare parametri ambientali e tracciare beni o attuatori mobili (ad esempio, trattori, droni, sensori remoti), sfruttando tecnologie di comunicazione a bassa potenza e garantendo un'infrastruttura economicamente efficiente. I risultati preliminari indicano una buona precisione di localizzazione anche in ambienti semi-strutturati e dinamici, dimostrando la resilienza al rumore e alle interferenze.

## Lorenzo Pisu

**Tema di ricerca:**

*Analisi, rilevamento e difesa da vulnerabilità web legate a nuove tecnologie.*

**Abstract**

Con l'avanzamento tecnologico delle moderne applicazioni web, i rischi di attacchi sia lato server sia lato client sono aumentati esponenzialmente. I dati e le funzionalità offerte dai siti web sono diventati sempre più centrali nella nostra vita quotidiana, dal settore sanitario a quello finanziario. Le vulnerabilità di questi servizi rappresentano oggi un potente strumento per gli attori malevoli, che riescono a esfiltrare dati sensibili e a compromettere il


Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

funzionamento degli applicativi, causando danni a imprese ed enti pubblici. Attraverso un'analisi sistematica delle tecnologie utilizzate dagli applicativi, è possibile individuare i rischi associati al loro utilizzo e definire strategie per ridurli o mitigarli. Partendo dallo studio delle modalità di attacco, si può arrivare a sviluppare difese automatiche capaci di bloccare gli utenti malevoli e impedire loro di sfruttare eventuali vulnerabilità. Questo progetto si concentra sulle tecnologie più recenti e innovative che, trovandosi ancora in una fase iniziale di adozione, possono presentare rischi maggiori proprio perché non ancora pienamente comprese. L'analisi parte dalla riproduzione sistematica di scenari d'uso vulnerabili, con l'obiettivo di costruire metodologie per riconoscere tali scenari anche in contesti reali. In molti casi, è possibile creare strumenti automatici in grado di individuare vulnerabilità su larga scala, permettendo così di misurare la diffusione di specifiche debolezze in applicativi web già in produzione.

## Cinzia Salis

**Tema di ricerca:**

*Sviluppo di un'interfaccia neurale bidirezionale impiantabile per il controllo protesico.*

**Abstract**

Attualmente si stima che vi siano oltre 40 milioni di amputati nel mondo, con circa 215.000 amputazioni eseguite ogni anno a causa di eventi traumatici o patologie croniche come diabete e tumori. Questi numeri sono destinati a crescere, complice l'invecchiamento della popolazione e la crescente incidenza di malattie come il diabete e le patologie cardiovascolari. In questo contesto, un settore di ricerca particolarmente promettente è quello volto al miglioramento della qualità della vita degli amputati attraverso lo sviluppo di protesi avanzate. Questi dispositivi mirano non solo al recupero motorio mediante il controllo tramite segnali elettromiografici (EMG), ma anche al ripristino del feedback sensoriale, con l'obiettivo di ricreare il senso del tatto. La percezione tattile, infatti, è indicata dagli amputati di arto superiore come una delle principali funzioni mancanti nelle protesi attualmente in commercio, che risultano spesso difficili da integrare nella vita quotidiana a causa dell'elevato carico cognitivo richiesto per il loro utilizzo. In letteratura esistono



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

principalmente due approcci per la realizzazione di dispositivi con elettrodi impiantabili. Il primo prevede l'interfacciamento tra i nervi e un dispositivo esterno tramite elettrodi impiantati e collegati con fili transcutanei. Questo metodo presenta diverse criticità, infatti i cavi che attraversano la pelle sono soggetti a danneggiamento e infezioni, e il dispositivo esterno risulta ingombrante e poco pratico per l'utilizzo quotidiano. Il secondo approccio si basa sull'impiego di protesi osteointegrate, che sfruttano un canale in titanio inserito all'interno dell'osso per il passaggio degli elettrodi, evitando così la necessità di connessioni percutanee. Tuttavia, questa soluzione non è adatta a una larga fetta di pazienti, in quanto condizioni come l'età avanzata, il diabete e l'osteoporosi, tra le principali cause di amputazione, precludono l'osteointegrazione. Il progetto di ricerca, quindi, propone di superare questi limiti attraverso lo sviluppo di un sistema costituito da un'unità di comunicazione centrale impiantabile, capace di ricevere dati e alimentazione in modalità wireless da un'unità esterna, e di comunicare tramite connessione cablata con diverse unità periferiche di neurostimolazione e acquisizione distribuite nel corpo. Questo approccio introduce due elementi fondamentali di avanzamento rispetto allo stato dell'arte. Il primo è la totale impiantabilità, che elimina il rischio di infezioni legate ai cavi transcutanei e rende il sistema più discreto e funzionale. Il secondo è quello di utilizzare un'architettura distribuita, che consente di posizionare l'unità centrale nel punto più accessibile dal punto di vista chirurgico, e i front-end di stimolazione e acquisizione direttamente in prossimità dei principali nervi o muscoli da stimolare o monitorare. Inoltre, l'adozione di front-end dedicati all'acquisizione di segnali EMG mediante elettrodi epimisiali (posizionati direttamente sul muscolo) consente un significativo miglioramento del controllo protesico, rendendo l'interazione con la protesi più naturale ed
efficace.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

**Davide Sitzia**

**Tema di ricerca:**

*Valutazione avanzata della qualità dei dati per il monitoraggio sincronizzato dei sistemi energetici.*

**Abstract**

Le attività di ricerca si concentrano sul miglioramento della qualità dei dati nel monitoraggio dei sistemi elettrici di potenza, con l'obiettivo di sviluppare tecniche avanzate applicabili anche al monitoraggio ambientale e ai segnali biomedici. Il nucleo del lavoro riguarda le misure sincronizzate nel tempo su ampie aree geografiche nei sistemi elettrici. In questo contesto, le Phasor Measurement Units (PMU) e le Merging Units (MU) sono dispositivi chiave: strumenti avanzati per l'osservazione in tempo reale della rete elettrica, la cui performance dipende non solo dalla qualità dell'hardware, ma anche dalle condizioni operative e dai meccanismi di sincronizzazione temporale. Per le PMU, la ricerca è dedicata alla caratterizzazione statistica degli errori di misura, con l'obiettivo di individuare i modelli più adatti a descriverne il comportamento. Inoltre, viene esplorata l'integrazione delle stime di sincròfasori con gli indici di qualità dell'energia elettrica, al fine di fornire un'indicazione sull'affidabilità delle misure. Parallelamente, le MU vengono studiate come elemento chiave nella catena di misura definita dallo standard IEC 61850, indagando l'introduzione di funzionalità intelligenti per il rilevamento automatico di eventi, anche in scenari rumorosi o complessi, sfruttando la tecnica del Matrix Profile (MP). Le metodologie sviluppate vengono quindi estese ad altri ambiti che condividono la sfida di effettuare misure affidabili in condizioni variabili.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

# XXXVII CICLO

## Chenhao Cui

**Tema di ricerca**

*Controllo cooperativo efficiente e migliorato della sicurezza di gru cingolate doppie con vincoli di movimento.*

**Abstract**

Le gru cingolate sono ampiamente utilizzate nei settori dell'energia eolica, della chimica e dell'edilizia, spesso per il sollevamento di attrezzature di grandi dimensioni come le pale delle turbine eoliche e le torri di distillazione. Con il continuo sviluppo di questi settori, il peso e la forma delle attrezzature da sollevare diventano sempre più complessi. Per i compiti che richiedono un'elevata precisione di installazione, come l'installazione di pale eoliche o di ponti, una singola gru è inadeguata a causa della sua capacità limitata e dell'incapacità di regolare la postura del carico, rendendo necessaria la collaborazione di due gru. Questa operazione di collaborazione aumenta significativamente la complessità e i rischi per la sicurezza del processo di sollevamento, che in genere richiede la collaborazione di più operatori esperti. Durante l'operazione, il percorso di sollevamento non può essere pianificato con precisione, richiedendo continui aggiustamenti vicino alla posizione di installazione per completare il compito. Questo approccio comporta un'incertezza significativa durante tutto il processo e porta a una bassa efficienza. Per raggiungere questo obiettivo, verrà creato un modello matematico ad alta fedeltà per caratterizzare le interazioni dinamiche tra gru doppie, carichi utili e fattori ambientali. Sfruttando questo modello, verranno progettate strategie di controllo per ridurre al minimo il tempo di ciclo e l'oscillazione del carico nei sistemi a doppia gru.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

## Hatami Davood

**Tema di ricerca:**

*Per sensori biochimici economici, portatili e affidabili basati su OFET.*

**Abstract**

Negli ultimi due decenni, i transistor organici a film sottile (OTFT) sono stati ampiamente studiati per applicazioni di rilevamento biochimico: dai sensori sensibili agli ioni a quelli enzimatici, immunologici e genetici. In questo campo, spinti in gran parte dalla richiesta di dispositivi a basso costo e monouso, adatti per lo screening su larga scala, varie architetture OTFT, come i transistor organici a effetto di campo elettrolitico (EGOFET), i transistor elettrochimici organici (OECT) e i transistor organici a effetto di campo a porta estesa (Ex-gate OFET), hanno guadagnato un'attenzione significativa nella comunità scientifica. Sebbene numerosi articoli abbiano riportato prestazioni notevoli e progressi tecnologici sostanziali, tra cui l'integrazione di materiali bidimensionali e lo sviluppo di piattaforme di sensori flessibili, trasparenti e completamente stampate, questi biosensori sono ancora confinati nei laboratori di ricerca. La loro limitata trasposizione in applicazioni reali continua a sollevare preoccupazioni per quanto riguarda l'affidabilità, la riproducibilità e la coerenza delle prestazioni dichiarate in condizioni operative pratiche.In questa tesi, si è cercato di fornire una valutazione più realistica dei vantaggi e dei limiti dei biosensori basati su OTFT. Particolare attenzione è stata dedicata ad affrontare i principali problemi di affidabilità che ostacolano il passaggio dalla ricerca di laboratorio alle applicazioni pratiche. Inoltre, sono state proposte potenziali strategie per affrontare queste sfide, con l'obiettivo di migliorare la stabilità, la riproducibilità e le prestazioni complessive di questi dispositivi in condizioni reali.

## Tianyu Liu.

**Tema di ricerca:**

*Sistemi Ciber-Fisici Sicuri e Affidabili: Modellazione, Analisi dell'Opacità e Diagnosi Temporale dei Guasti mediante Automi a Uscita Commutabile.*



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

**Abstract**

I sistemi cyber-fisici (CPS) le cui uscite sono segnali discreti o continui quantizzati richiedono formalismi di modellazione in grado di catturare simultaneamente il comportamento logico e le informazioni temporali. Gli Switching Output Automata (SOA) soddisfano questo requisito associando a ogni stato discreto un insieme finito di possibili valori di uscita e imponendo un tempo di permanenza minimo che previene i fenomeni di Zeno. Questa tesi sviluppa un framework incentrato sui SOA che porta avanti due filoni di ricerca complementari: la sicurezza del flusso di informazioni, affrontata attraverso l'analisi dell'opacità, e l'affidabilità, affrontata attraverso la diagnosi dei guasti. Per quanto riguarda la sicurezza, la tesi stabilisce innanzitutto condizioni e algoritmi rigorosi per la verifica dell'opacità dello stato corrente (Current-State Opacity, CSO), garantendo che un osservatore esterno non possa dedurre stati segreti dagli output osservabili. L'approccio si basa sulla costruzione sistematica di automi di evoluzione e dei loro osservatori, consentendo un'analisi scalabile. Il concetto viene poi generalizzato all'opacità temporale, in cui i segreti sono definiti non solo dallo stato globale ma anche dal tempo di permanenza in quello stato. Le astrazioni logiche che discretizzano il tempo in un numero finito di intervalli conservano tutte le informazioni necessarie per il compito di verifica. Per quanto riguarda l'affidabilità, il lavoro introduce gli automi a commutazione di uscita con guasti (SOAF) e l'automa a evoluzione con guasti (EAF) associato. Questo formalismo modella guasti la cui occorrenza è vincolata a finestre temporali che dipendono sia dallo stato discreto sia dall'uscita corrente. Adattando la sintesi classica di un diagnoser, la tesi deriva un diagnoser temporizzato in grado di rilevare e isolare tali guasti. La praticità della modellazione basata su SOA e della verifica CSO è dimostrata su un sistema di approvvigionamento idrico intelligente di riferimento, evidenziando il potenziale del framework per la security-by-design nelle infrastrutture reali. I risultati teorici sull'opacità temporizzata e sulla diagnosi temporizzata dei guasti gettano le basi per la prossima validazione e integrazione sperimentale, con l'obiettivo finale di migliorare sia la sicurezza che l'affidabilità di CPS complessi.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

**Gao Jie**. (co-tutorship: Northwestern Polytechnic University, Xi'an, China)

**Tema di Ricerca:**

*Studio sull'algoritmo di rilevamento di video deepfake facciali.*

**Abstract:**

La tecnologia “deepfake”, emersa nel 2017, è una forma sofisticata di manipolazione facciale che può essere utilizzata per scopi malevoli alterando le espressioni facciali o le identità. Numerose applicazioni “deepfake”, come FakeAPP e ZAO, sono diventate ampiamente disponibili. Con la continua evoluzione della tecnologia Deepfake, i contenuti generati diventano sempre più realistici. Queste tecnologie guidate dall'intelligenza artificiale offrono nuove possibilità di creare immagini e video falsi di alta qualità, che rappresentano una minaccia significativa per la privacy personale, la reputazione sociale e la sicurezza nazionale. Sebbene siano stati proposti diversi metodi di rilevamento dei Deepfake, esistono ancora sfide irrisolte in questo campo. Ciò evidenzia l'urgente necessità di tecniche di rilevamento Deepfake efficaci per affrontare le gravi sfide poste dai contenuti visivi falsi. Questo dottorato si concentra sul rilevamento di Deepfake facciali, affrontando in particolare questioni come i problemi di compressione, la generalizzazione di casi trasversali e altre sfide correlate. L'obiettivo è quello di alleviare questi problemi esplorando soluzioni innovative per migliorare il rilevamento dei contenuti Deepfake.

**Wenjie Zhao**. (Co-tutorship: Xidian University, Xi'an, China).

**Tema di Ricerca:**

*Controllo e Mantenimento della Connettività Algebrica con Applicazione alle Reti Aperte di Multi-Agenti.*

**Abstract:**

La ricerca mira a progettare protocolli distribuiti per migliorare la resilienza delle reti variabili nel tempo contro la disconnessione in reti aperte multi-agente. In tali reti aperte, gli agenti



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

possono dinamicamente unirsi, abbandonare, fallire o subire attacchi alla rete come attacchi Denial-of-Service (DoS) o False Data Injection (FDI). I metodi proposti si basano sull'auto-organizzazione della struttura del grafo della rete, utilizzando solo informazioni locali o informazioni stimate a livello globale (comprese le proprietà spettrali della matrice laplaciana corrispondente) ottenute tramite algoritmi di consenso e ottimizzazione distribuiti. L'obiettivo è ottimizzare la topologia della rete verso una forma strutturale desiderata con il minimo numero di azioni. Idealmente, la rete dovrebbe mantenere un'elevata connettività algebrica rispettando un determinato vincolo di grado desiderato (il numero di bordi/canali di comunicazione per agente). I protocolli sviluppati in questa ricerca saranno applicabili a sciami di veicoli aerei senza pilota (UAV), reti peer-to-peer su larga scala di utenti anonimi e reti multi-agente su larga scala che interagiscono attraverso infrastrutture di comunicazione. Questi metodi miglioreranno in modo significativo la resilienza di questi sistemi contro le disconnessioni. Inoltre, questa ricerca esplorerà le tecniche per ottenere topologie di grafi r-robuste attraverso l'auto-organizzazione. Ciò consentirà l'applicazione pratica di garanzie formali per la convergenza e la stabilità dei protocolli distribuiti basate su condizioni grafo-teoriche, dove la robustezza r è un indicatore critico della resilienza di un sistema in rete agli attacchi IDE.

# XXVI CICLO

**Tenglong Kang**. (co-tutorship: Xidian University, Xi'an, China)

**Tema di Ricerca:**

*Diagnosi dei guasti dei sistemi a eventi discreti sotto attacco dei sensori.*

**Abstract:**

Lo studio riguarda il problema di diagnosticare il verificarsi di un evento di guasto in un sistema a eventi discreti (DES) soggetto ad attacchi malevoli. Consideriamo un DES monitorato da un operatore attraverso le osservazioni percepite dai sensori. Si ipotizza che esista un attaccante attivo in grado di manomettere le osservazioni dei sensori ricevute



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

dall'operatore del sistema. A questo proposito, introduciamo la nozione di diagnosticabilità robusta contro gli attacchi, per cogliere la capacità dell'operatore di diagnosticare comunque l'occorrenza di guasti in caso di attacchi. Per verificarla, proponiamo la nozione di verificatore e di diagnosi congiunta sotto attacco, sulla base della quale viene presentata una condizione necessaria e sufficiente per la diagnosticabilità robusta. Si dimostra che l'approccio proposto, basato sul verificatore, richiede un tempo polinomiale rispetto al numero di stati ed eventi di un sistema. D'altra parte, rispetto al verificatore sotto attacco, la diagnosi congiunta può essere utilizzata per verificare se un attaccante può non essere scoperto dall'operatore del sistema, cioè mantenersi furtivo. Il diagnoser raffinato, chiamato diagnoser congiunto furtivo, fornisce una condizione necessaria e sufficiente per l'esistenza di un attaccante di successo, che può distruggere la diagnosticabilità e nel frattempo mantenersi furtivo.

**Kun Peng**. (co-tutorship: Xidian University, Xi'an, China)

**Tema di Ricerca:**

*Approccio di sintesi per l'applicazione dell'opacità mediante controllo di supervisione e funzione di editing.*

**Abstract:**

L'opacità è una proprietà cruciale nei sistemi sensibili alla sicurezza, in quanto impedisce l'inferenza non autorizzata di informazioni riservate. In un sistema a eventi discreti (DES), le informazioni segrete possono essere classificate in un insieme di stati e in un linguaggio, che classificano la proprietà in opacità basata sullo stato e opacità basata sul linguaggio, rispettivamente. I vari tipi di opacità basata sullo stato includono l'opacità dello stato iniziale, l'opacità dello stato attuale, l'opacità iniziale-finale, l'opacità dello stato ritardato K e l'opacità dello stato infinito, definiti in base ai tipi di stato segreto o alla tempestività delle informazioni riservate. I tipi di opacità sopra menzionati possono essere trasformati in opacità allo stato attuale, che è la più semplice da verificare e da applicare con i


Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it

corrispondenti tipi di monitoraggi segreti. Costruendo gli osservatori di stato corrente dei monitor, possiamo verificare se l'impianto originale soddisfa il tipo di opacità richiesto. In caso contrario, possiamo cercare il linguaggio che viola il tipo di opacità. Per imporre l'opacità dell'impianto originale, possiamo adottare il metodo del controllo di supervisione per disabilitare questi comportamenti o corrompere l'osservazione di un intruso per impedirgli di dedurre questi comportamenti. Per un caso più pratico, esiste un insieme di eventi controllabili, un insieme di eventi cancellabili e un insieme di eventi inseribili, il che implica che alcuni comportamenti illegali non possono essere disabilitati o modificati e che l'applicazione dell'opacità non può essere realizzata adottando solo funzioni di controllo di supervisione o di modifica. Sintetizziamo i due metodi per proporre un approccio innovativo in grado di soddisfare un maggior numero di casi.



Segretario amministrativo: Dott. Luigi Giordano
Via Marengo 2 – Cagliari
Tel +39 070/6756647 – email segreteriadiee@unica.it
www.unica.it