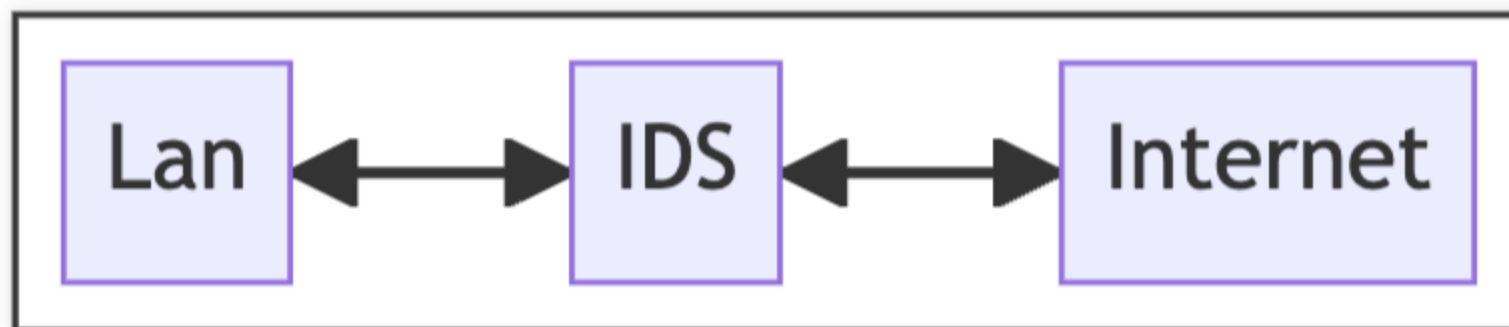


Utilizzo di Soft-Brownian-Offset per la generazione di attacchi ai fini dell'addestramento di rilevatori di intrusioni

INTRUSION DETECTION SYSTEMS (IDS)

Applicazione che monitora continuamente la rete per identificare attività malevole.



Nell'ultimo decennio si è iniziato ad utilizzare algoritmi di
Machine Learning per gli IDS.

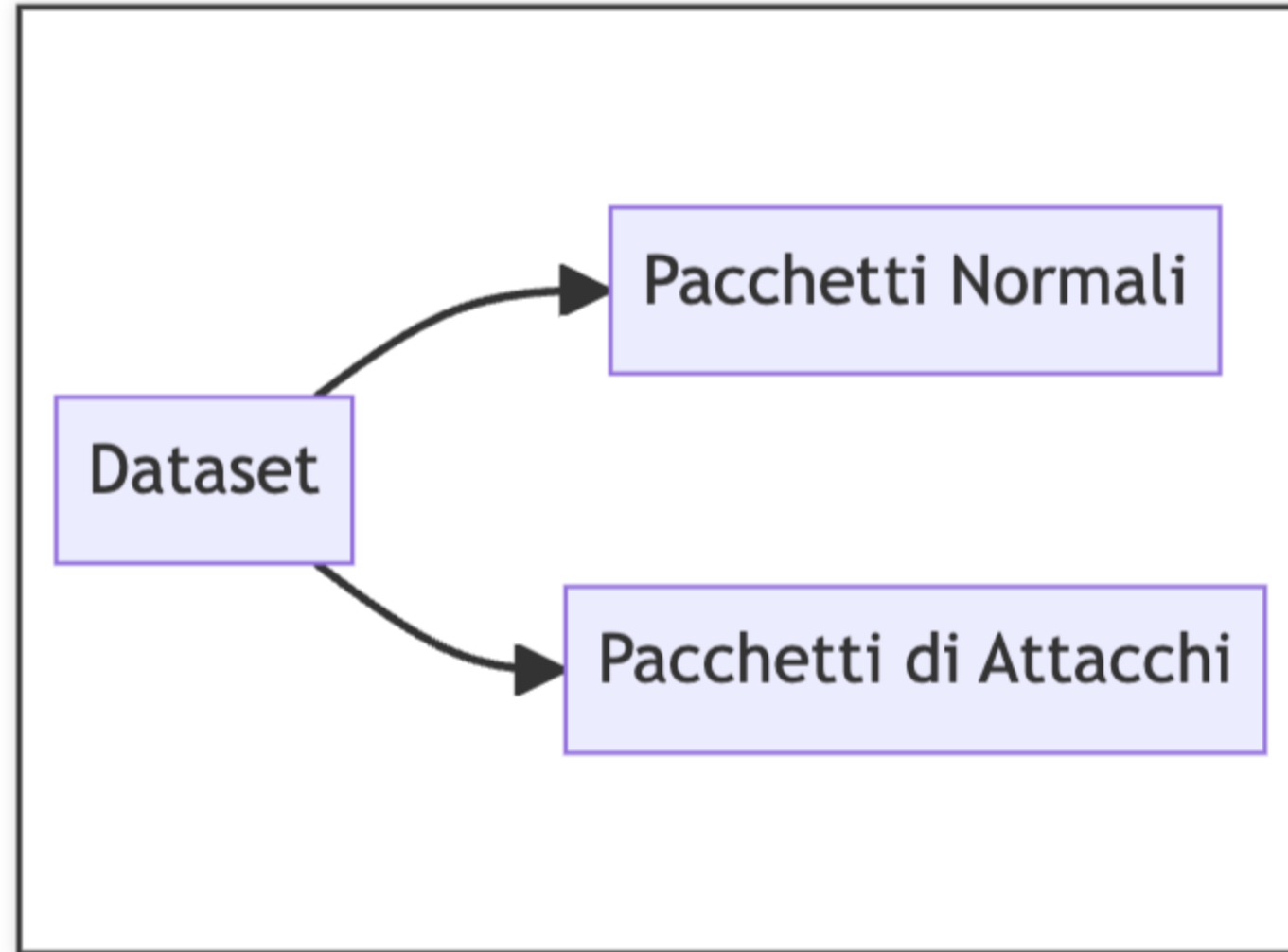
MACHINE LEARNING

La branca dell'**Intelligenza Artificiale** che sviluppa modelli per permettere alle macchine di imparare dai dati.

PROBLEMA

I modelli di Machine Learning sono sensibili ai dati di addestramento.

DATASET DI UN IDS



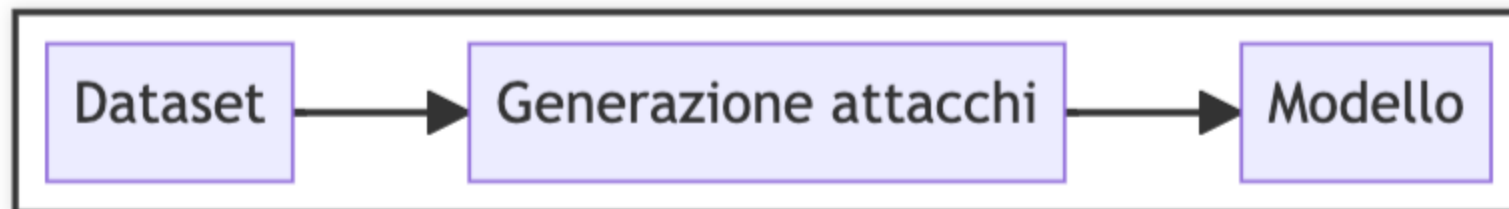
UNA SOLUZIONE

Generare nuovi dati a partire da quelli già esistenti per migliorare i modelli di Machine Learning

- Soft-Brownian-Offset

SCOPO DELLA TESI

Cercare di migliorare un IDS utilizzando Soft-Brownian-Offset



SOFT BROWNIAN OFFSET

Algoritmo di generazione di dati creato inizialmente per la generazione di eventi anomali.

DATASET UTILIZZATI

- Adfanet
- CICIDS

APPROCCI DI GENERAZIONE

Generazione a partire dalla tipologia di dati:

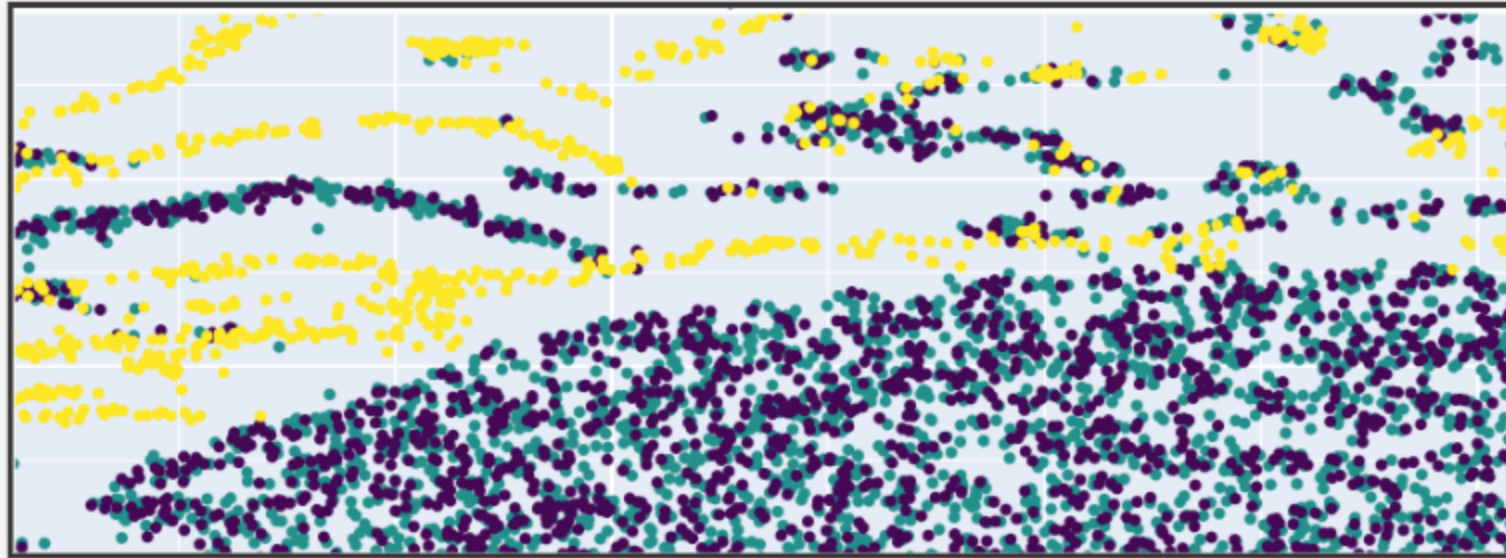
- Solo pacchetti normali
- Solo pacchetti attacchi
 - Dataset completo

GRAFICI

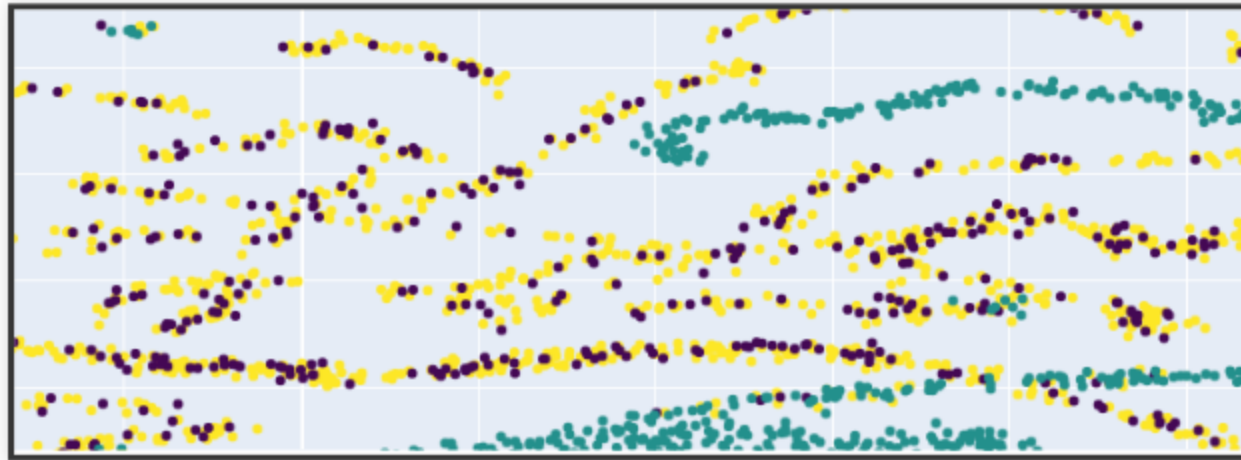
Per una valutazione qualitativa degli approcci di generazione.

GENERAZIONE

A PARTIRE DA PACCHETTI NORMALI



GENERAZIONE A PARTIRE DA PACCHETTI DI ATTACCHI



APPROCCI DI ADDESTRAMENTO DEL MODELLO

Addestramento usando:

- Dataset completo + Dati sintetici
- Solo pacchetti normali + Dati sintetici
- Solo dataset (senza dati generati)

ADFANET

	Pacchetti normali + Gen	Dataset Completo + Gen	Solo Dataset
Gen Normali	0.3337	0.99839	0.93596
Gen Attacchi	0.4404	0.99865	0.93596
Gen Completo	0.3452	0.99854	0.93596

ADFANET

	Pacchetti normali + Gen	Dataset Completo + Gen	Solo Dataset
Gen Normali	0.3337	0.99839	0.93596
Gen Attacchi	0.4404	0.99865	0.93596
Gen Completo	0.3452	0.99854	0.93596

CICIDS

	Pacchetti normali + Gen	Dataset Completo + Gen	Solo Dataset
Gen Normali	-0.1153	0.92772	0.93596
Gen Attacchi	-0.1366	0.93428	0.93596
Gen Completo	-0.1206	0.92493	0.93596

CICIDS

	Pacchetti normali + Gen	Dataset Completo + Gen	Solo Dataset
Gen Normali	-0.1153	0.92772	0.93596
Gen Attacchi	-0.1366	0.93428	0.93596
Gen Completo	-0.1206	0.92493	0.93596

CONCLUSIONI

Soft Brownian Offset è efficace nel caso di dataset **semplici**.

In dataset **complessi** invece l'algoritmo non presenta miglioramenti.

In quest'ultimo caso è necessario rivolgersi ad algoritmi differenti.

GRAZIE PER L'ATTENZIONE