Internet of Things: rilevare attacchi informatici mediante analisi del consumo energetico

Tesi di Laurea in

Ingegneria Informatica

Candidato
Giorgio Cecchi

Relatori
Prof. Alessio Vecchio
Prof. Pericle Perazzo

UNIVERSITÀ DI PISA

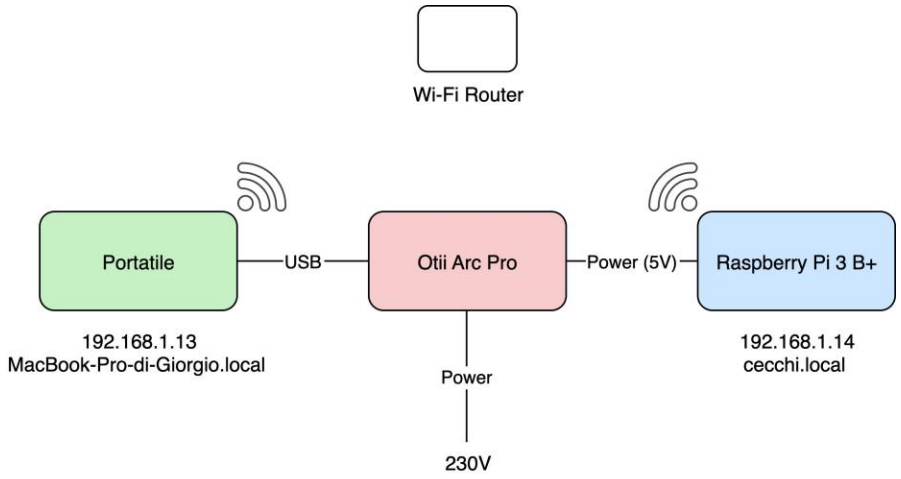
Introduzione e Problema

- I dispositivi IoT sono largamente usati in vari contesti e sono in numero estremamente elevato (in continuo aumento)

- Problema
  - Tali dispositivi sono fortemente eterogenei e hanno risorse limitate, pertanto non si prestano alle soluzioni di sicurezza tradizionali (antivirus, antispyware, …)
  - Come si garantisce la sicurezza di questi dispositivi senza impattare sulle performance?

Soluzioni

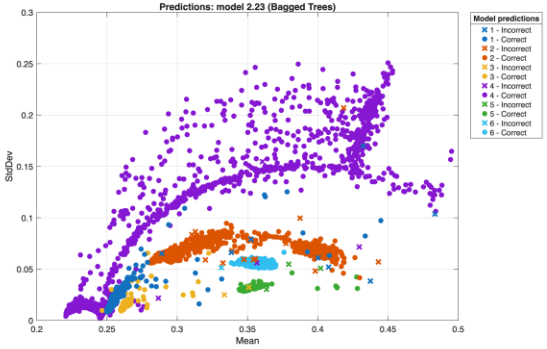
- Analizzando il consumo energetico di un dispositivo si possono individuare particolari pattern relativi ad un certo processo, quindi è possibile individuare eventuali pattern relativi a processi riguardanti attività malevole
- Abbiamo monitorato il consumo di un Raspberry Pi 3 Model B+ con un Otii Arc Pro durante tre attività normali e tre malevole.
  1) Sensore
  2) Camera Smart
  3) Server Web
  4) Attacco Bruteforce SSH
  5) Attacco DoS DNS
  6) Attacco DoS HTTP

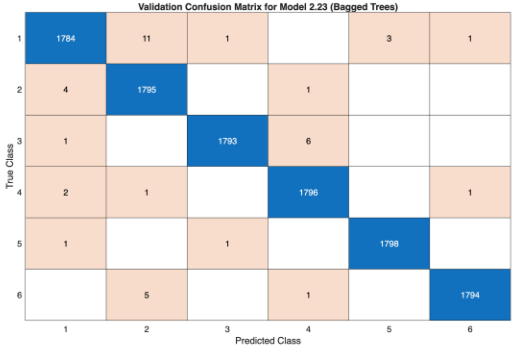


- Successivamente abbiamo addestrato algoritmi di machine learning a classificare tali attività.

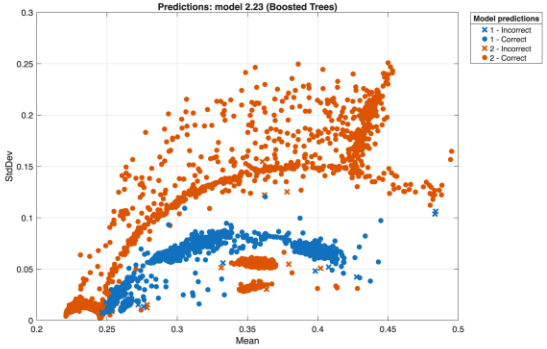
Risultati

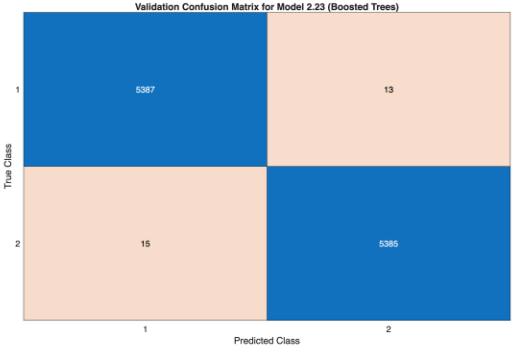
- Scenario 1: classificazione multi-classe ⇨ Accuratezza > 99%





- Scenario 2: classificazione binaria ⇨ Accuratezza > 99%





- Scenario 3: classificazione binaria, training con soli dati normali

  ⇨ Recall (individuazione attività malevole) > 90%