UNIVERSITY OF CAPE TOWN
IYUNIVESITHI YASEKAPA • UNIVERSITEIT VAN KAAPSTAD

ACKERSON Emmanuel
Supervisor: Dr. Josiah Chavula

HPI Hasso Plattner Institut

Intrusion Detection Reliability in Software Defined-Community Wireless Networks

INTRODUCTION

Community Wireless Networks (CWNs) provide easy and cost-effective internet access to underserved communities that lack the economic advantage to attract and afford the services offered by Internet Service Providers (ISPs). Nevertheless, its unique architecture and resource constraints pose security vulnerabilities that are easily exploitable.

Images illustrating CWN, its benefits and associated security vulnerabilities

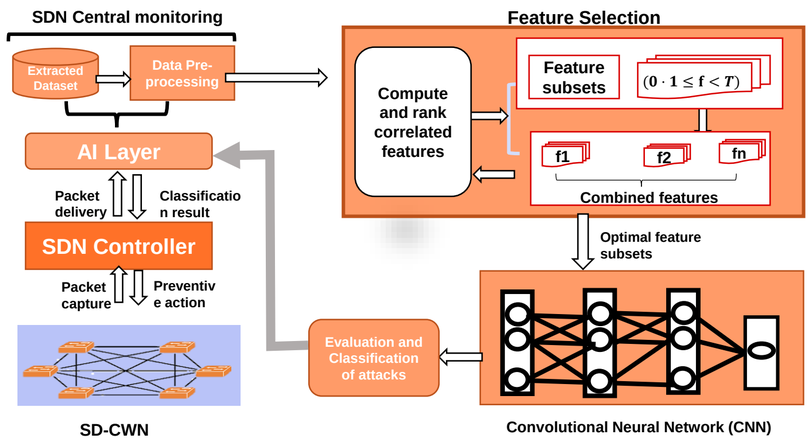
THE OBJECTIVE

Design and implement efficient and effective IDS mechanism for constrained networks:

- Deep analysis of CWN dataset to gain insight into malicious activities
- Employ ML/DL techniques and SDN architecture to design resource efficient IDS for low-resource CWNs

THE SOLUTION ARCHITECTURE

SDN and ML/DL techniques to improve network monitoring, enhance data collection, and enable optimised feature extraction.



SD-CWN Physical Layer
- Facilitate data distribution within the network. gathers statistical data regarding network behaviour

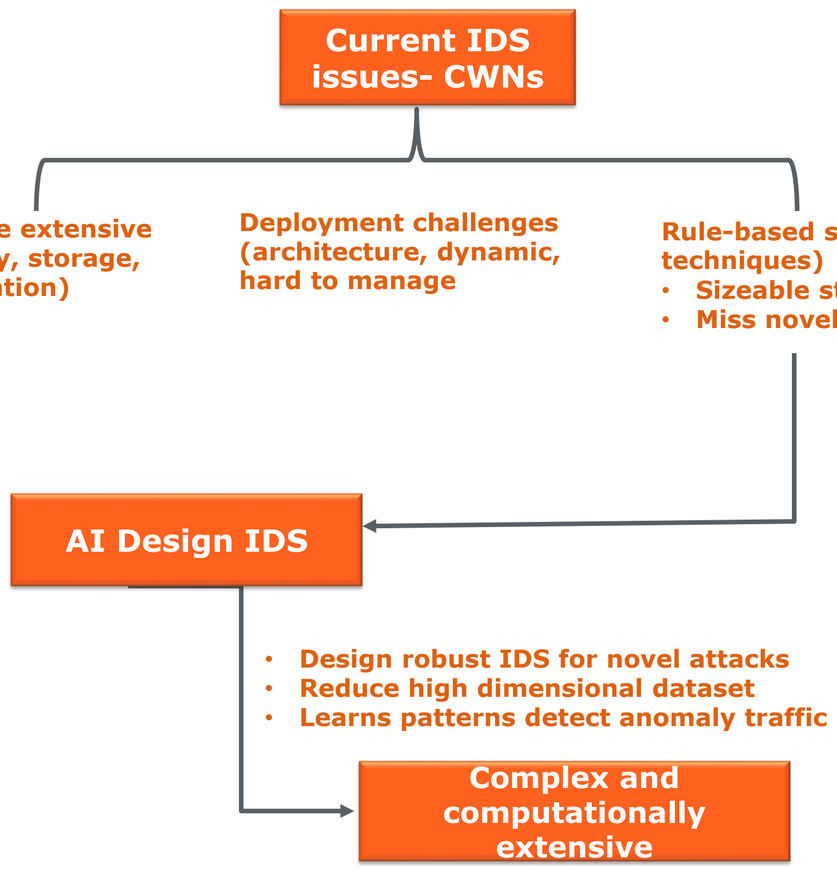
SDN Controller
- Monitors and manages network behaviour. Captures and extracts statistical information for AI layer

ML Feature Selection
- CFS ranks and eliminates correlated features from dataset. Combines features. Selects optimal subsets.

DL Classification Model
- CNN DL classifies, evaluate and detects attacks. Classification outcome sent to management layer via AI layer for preventive action

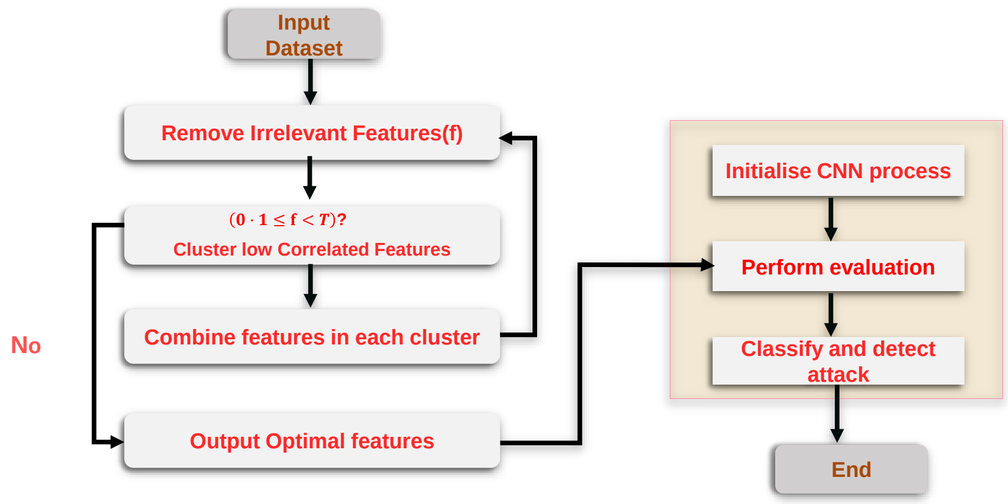
Security Mechanisms and challenges to CWNs

Current security measures, particularly intrusion detection systems (IDSs), are primarily tailored for conventional networks. Hence, less unsuitable for low-resource CWNs, thereby creating deployment challenges.



Extraction of Informative features from datasets for ML-IDS modeling is computationally extensive, time consuming and resource costly.

Algorithm of proposed ML-IDS modeling design for CWNs environment



PCC;
- compute and rank features (f).
- eliminate highly-correlated features

Clustering;
- Group lowly-correlated feature subsets below threshold T.

Concatenation;
- Combine each group of lowly correlated features

CNN;
- Analyses and evaluates features
- Classifies and detect malicious attacks

Scientific Contributions

- **Utilisation of real-world CWN dataset to gain in-depth understanding of application behaviour and network activities, including identification of potential anomalies.**
- **Establishment of a foundation reference pertaining to malicious activities in CWNs through empirical analysis.**
- **Application of filter-based correlation as exclusive FS procedure to improve performance of classifier models**
- **Design and implementation of an CWNs -specific IDS mechanism that optimises network resources, and management**

References

1. Anomaly detection for abnormal detection in CWNs – L. Cerda-Alabern et. al (2023)
2. Enabling entrusted security for CWMNs – Neuman et. al (2018)
3. Mobile and active IDS for IEEE 802.11s WMNs – Rodrigo do Carmo et. al (2018)
4. Two-Phase Hybrid FS IDS – Huang et al (2018)
5. Design and analysis of IDS for WMNs – Al-Anzi et. al (2022)
6. Fussion of Statistical importance -Thakker et al (2023)
7. IDS for multimeasure FS for Fog Environment - Huang et al (2023)