ROUT-4-2023: RPL Based Routing Attack Dataset for IoT

This dataset consists of .csv files of 4 different routing attacks (Blackhole Attack, Flooding Attack, DODAG Version Number Attack and Decreased Rank Attack) targeting the RPL protocol and these files are taken from Cooja (Contiki network simulator). It gives researchers the opportunity to develop IDS for RPL-based IoT networks using Artificial Intelligence and Machine Learning methods without simulating attacks. Simulating these attacks is an important step towards developing and testing protection mechanisms against such attacks by mimicking real-world attack scenarios. For these researchers, it may offer an alternative approach to intrusion detection systems that have limitations of traditional methods. This requires identifying appropriate attributes that include characteristics of attacks, analyzing network traffic data, and considering other relevant parameters. It is also important that your dataset is balanced and representative so that your model can accurately identify and predict different types of attacks. In conclusion, this study is an important step in the field of IoT security. By simulating four different routing attacks to IoT devices through Cooja, we present a new dataset to detect attacks for application in artificial intelligence and machine learning methods.

Table1: Features of CSV files

Name/Abbreviation	Description
TIME	Simulation time
SOURCE	Source Node IP
DESTINATION	Destination Node IP
LENGTH	Packet Length
INFO	Packet Information
TR	Transmission Rate(per 1000_ms)
RR	Reception Rate(per 1000 ms)
TAT	Transmission Average Time
RAT	Reception Average Time
TPC	Transmitted Packet Count(per second)
RPC	Received Packet Count(per second)
TTT	Total Transmission Time
TRT	Total Reception Time
DAO	DAO Packet Count
DIS	DIS Packet Count

DIO	DIO Packet Count
CATEGORY	Attack Type or Normal
LABEL	Normal/Malicious Label