ISOT Drone Anomaly Detection Dataset

The password for the archive is: drone

ISOT Drone Anomaly Detection Dataset contains 14 hours of anomalous data and 10 hours of benign data. All the captured data is considered raw data in the PCAP format and then extracted into a dataset in CSV files.

Data Type	Attack Vector	Sub-Categories	PCAP file size	CSV file size
Benign Data	N/A	N/A	14.7 GB	649 MB
Anomalous Data	Deauthentication Attack	N/A	548 MB	116 MB
	DoS Attacks	TCP flood	439 MB	119 MB
		Slowloris	1.46 MB	851 KB
		SlowHTTPTest	11.9 MB	5 MB
		Hulk	19.9 MB	9 MB
		UDP flood	5.76 GB	338 MB
	MITM Attacks	drone network	1.23 GB	47.7 MB
		Station Mode	15.9 MB	4 MB
	Inject Instructions	N/A	8 MB	2.36 MB
	Video Interception Attack	N/A	995 MB	38.2 MB
	Replay Attack	N/A	4.46 MB	2.52 MB
	Payload Manipulation	N/A	4.57 MB	2.7 MB
	Unauthorized UDP Packets	N/A	9.3 MB	2.47 MB
	IP Spoofing	N/A	7.27 MB	4.49 MB

Table 1. Overview of the Data Files

The dataset is generated based on a variant of the original CIC IoT scripts. It provides a balanced dataset of benign and anomaly data, totaling 1.2 million and 1.6 million samples, respectively. The modifications to the original scripts are:

New	Removal	Modification
Payload Length	Flow_duration	DS Status
Drone_port	Header_length	Drate and Srate
Entropy	MAC	Rate
Variance of Payload	Protocol Version	Inter-Arrival Time

Table 2. Feature Set Modification

References

To cite this dataset use:

Z. Chen, I. Traoré, M. Mamun, and S. Saad, "Drone Anomaly Detection: Dataset and Unsupervised Machine Learning", International Symposium on Foundations & Practice of Security (FPS 2024), Montréal, Canada, Dec. 9, 2024.