1. Real time NIDS using deep learning
2. Feature learning on raw network traffic heads instead of derived features.
3. IDS to detect other types of attacks against the IoT including location dependent attacks such as cloning of device ID, spooﬁng, and sybil attacks also for zero-day attacks [1].
4. Limited features were used [2].

[1] https://www.mdpi.com/1424-8220/19/9/1977/pdf';google.navigateTo(parent,window,redirectUrl);})();</script> <noscript> <META content="0;URL=https://www.mdpi.com/1424-8220/19/9/1977/pdf

[2] https://pdfs.semanticscholar.org/a30c/16f5598ba18ffd7d9c533515cf671d54b382.pdf