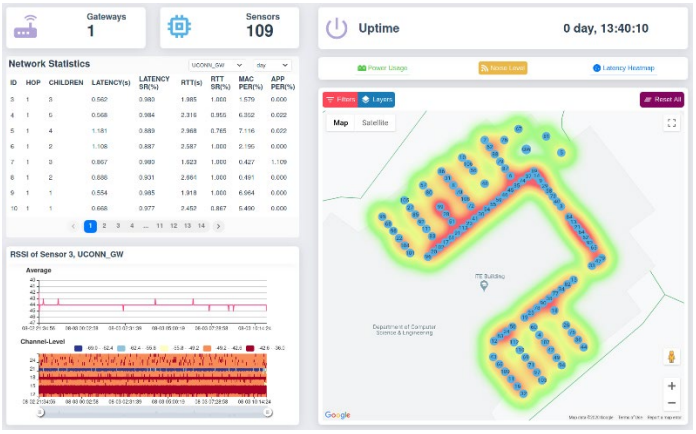
Network Anomaly Detection in 6TiSCH Networks

Jiachen Wang, Song Han, Computer Science and Engineering Department
University of Connecticut

The past decade has witnessed the rapid development of real-time wireless technologies and their wide adoption in various industrial Internet-of-Things (IIoT) applications. Among these technologies, 6TiSCH (IPv6 over the TSCH mode of IEEE802.15.4e) is a promising candidate as the de facto standard due to its nice feature of gluing a real-time link-layer standard with an IP-enabled upper stack for seamless integration with Internet services. However, as a typical IIoT network that runs on resource constrained devices, 6TiSCH cannot directly apply modern (and computation-intensive) security mechanisms. How to protect packets from tampering and eavesdropping for such network with low cost is a great challenge. To this end, we proposed a machine-learning based anomaly detection mechanism for 6TiSCH network. Our approach is to learn the network traffic pattern and build a link fingerprint database. Thanks to the TSCH feature of 6TiSCH network, we have 16-dimension channel-level link quality data for training the model. This significantly improve our accuracy. We tested the approach on the 6TiSCH testbed at University of Connecticut (UConn), which to our best knowledge is the largest operational 6TiSCH network in U.S.. The results show that on a 100-device static network, with 2-day data we can recognize each link with 99.72% accuracy.



Acknowledgements: This project was financially sponsored by Transportation Infrastructure Durability Center (TIDC).

References

[1] X. Vilajosana, T. Watteyne, M. Vuˇcini´c, T. Chang and K. S. J. Pister, ”6TiSCH: Industrial Performance for IPv6 Internet-of-Things Networks,” in Proceedings of the IEEE, vol. 107, no. 6, pp. 1153-1165, June 2019.
[2] Chalapathy, Raghavendra, and Sanjay Chawla. "Deep learning for anomaly detection: A survey." arXiv preprint arXiv:1901.03407 (2019).