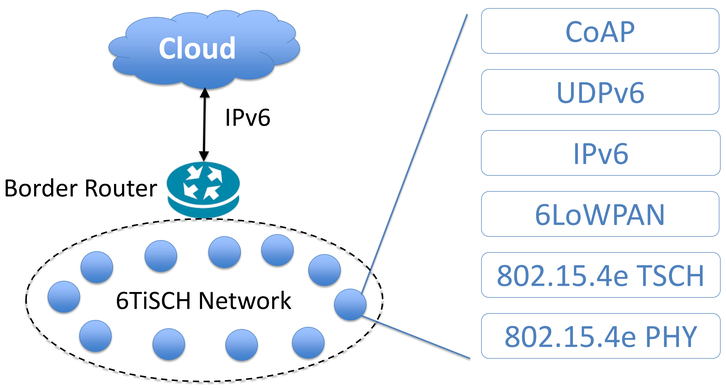
# Network Anomaly Detection in 6TiSCH Networks

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

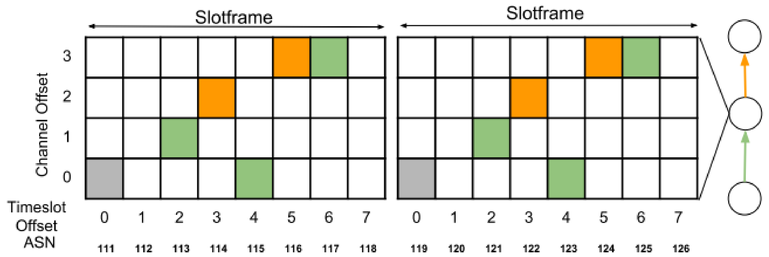
## 6TiSCH Network

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 runs on resource constrained devices, 6TiSCH networks cannot directly apply the modern (and computation-intensive) cryptography-based security mechanisms. How to protect packets from tampering and eavesdropping for such network with low cost is a great challenge.




The 6TiSCH architecture and stack




Time Slotted Channel Hopping (TSCH)

## TSCH Fingerprinting

A common attack scenario for IIoT network is:

- Sneak into the industrial infrastructure.
- Deploy a malicious device.
- Tamper the sensing/control packets.

Since the malicious device is in a different place from normal devices, the noise and link quality must be different. Then we can find the attacker's device by detecting unrecognized links.

A key feature of 6TiSCH network is the time-slotted channel hopping (TSCH), which enable the devices use different channels (up to 16 channels) at different time. Besides the extreme reliable performance, this channel hopping also offers us a 16-dimension feature to model a link!

With such high dimension and interpretable feature, we can build a link fingerprint database and detect network anomalies with a very high accuracy. Then we can protect the IIoT networks from outside attackers in a low cost (without cryptography).


6TiSCH testbed @ UCONN

## Experiment Results

We have tested our link-fingerprint based anomaly detection approach on our 6TiSCH testbed at UCONN, which to our best knowledge is the largest operational 6TiSCH network in U.S. with more than 120 devices. The results shows on a static network, with 2-day's traffic data, we can recognize each link with 99.72% accuracy.

About future work, we will keep exploring more available features and machine learning models to improve the accuracy, as well as the emergency respond speed.