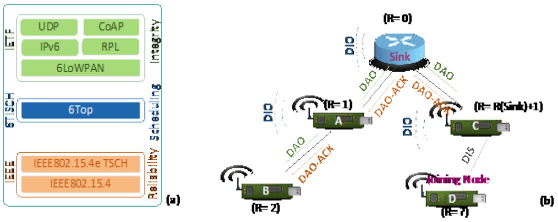
Detecting Routing Attacks in Industrial Internet of Things Systems

Areej Althubaity, Song Han, Computer Science and Engineering Department
University of Connecticut

Abstract

Over the last decade, the advanced technologies in the wireless communication enabled hundreds of small sized battery-operated devices to form a network where they share their information with the Internet; hence the term Internet of Things (IoT) have been born. Due to their ease of deployment, low cost, and wired-like connectivity, the wireless communication looks like a good candidate to be adapted to the industrial applications, but they had to go under major improvements to be acceptable for the industrial high performance requirements and thus the Industrial IoT (IIoT) terminology have been evolved. However, the routing protocol that specifies for devices how they can communicate with each other have been targeted by internal attacks that designed to disrupt the networks. Since the devices in such networks are usually limited in the storage space, and processing power and also most of them are battery operated, they can be easily re-programmed to act maliciously. In our research project, we design Intrusion Detection Systems (IDSs) to detect internal routing attacks that cannot be detected through any scruirty primitives and prevent them from manipulating the networks and cause any severe damage to the devices connectivity. Our IDSs do not require any high computation power, demand huge storage space, or drain energy from the devices which make them lightweight suitable for the Industrial IoT.



(a) Overview of the 6TiSCH architecture; (b) an example of an RPL routing graph

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

References

[1] A. Althubaity, H. Ji, T. Gong, M. Nixon, R. Ammar, and S. Han, ARM: A hybrid specication-based intrusion detection system for rank attacks in 6tisch networks," in 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2017.

[2] A. Althubaity, T. Gong, K. R. Choo, M. Nixon, R. Ammar, and S. Han, Specification-based distributed detection of rank-related attacks in rpl-based resource-constrained real-time wireless networks," in the 3rd IEEE International Conference on Industrial Cyber-Physical Systems (ICPS 2020), 2020.