Cyber-Physical Fingerprinting for Internet of Things Authentication: Accelerating IoT Research and Education Under the Global City Teams Challenge

VT: Walid Saad (PI), Sanjay Raman (co-PI)

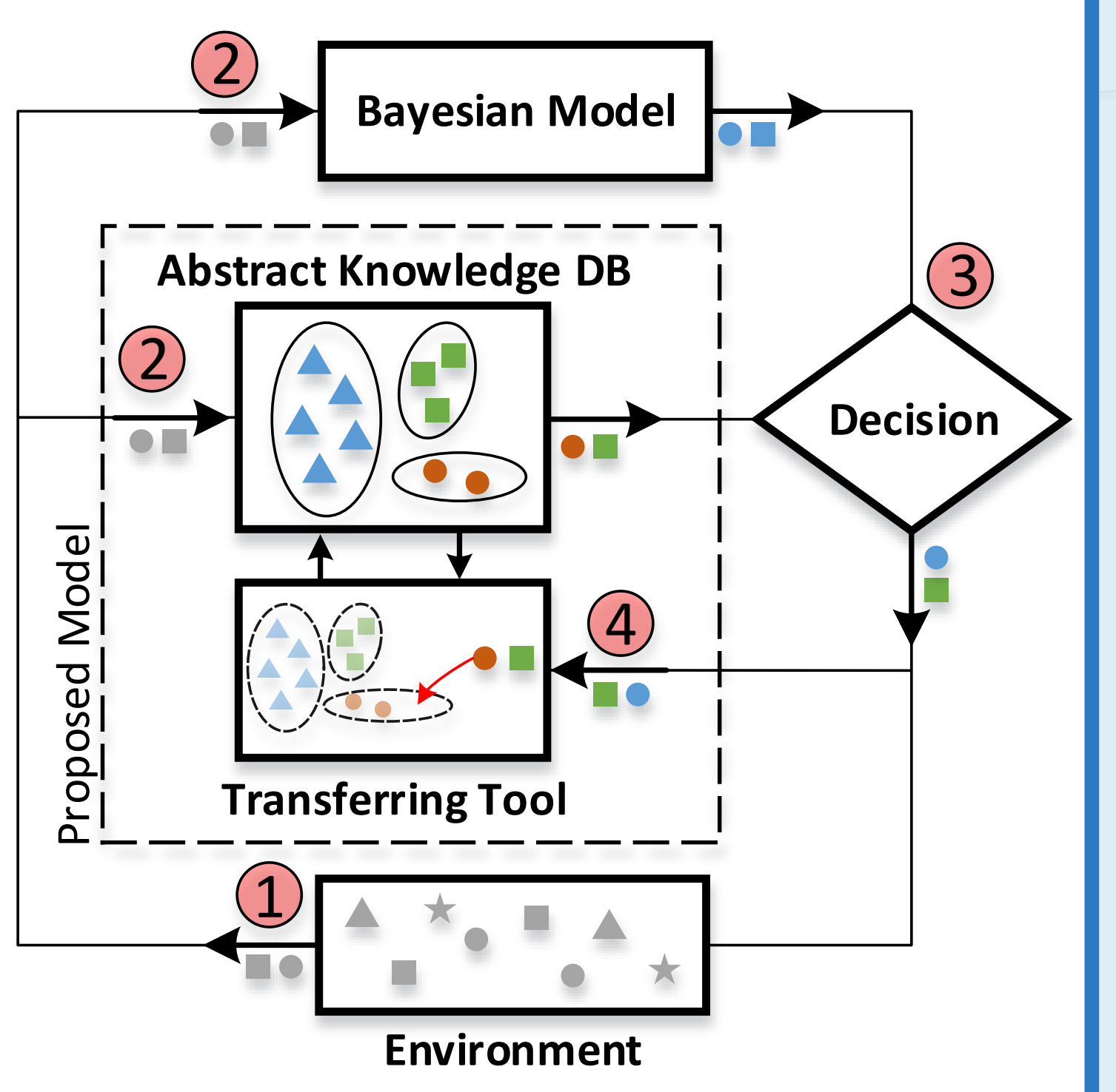
Transfer Learning for Device Fingerprinting with Application to Cognitive Radio Networks

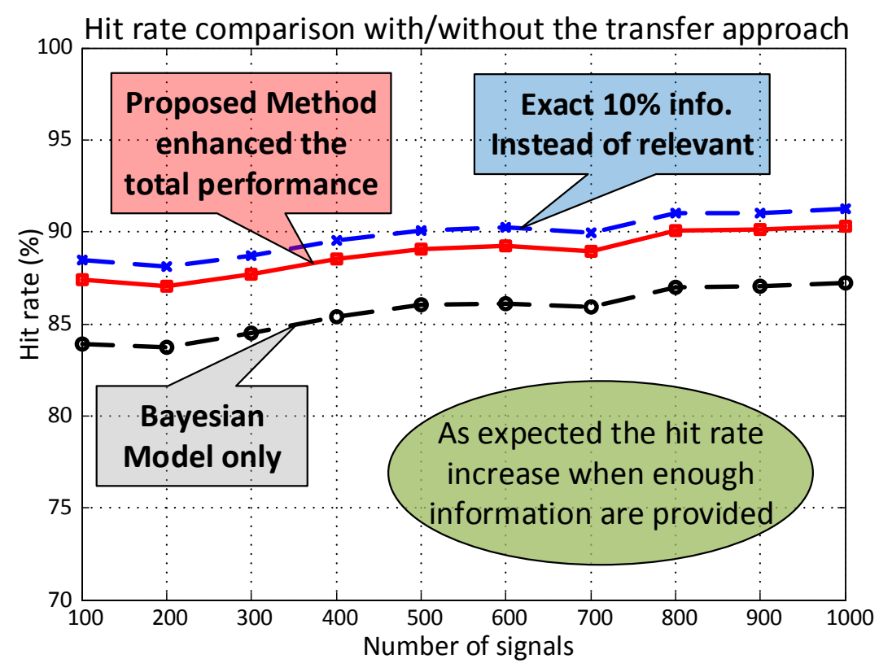
The paper received a "Best Paper Award" at International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*.

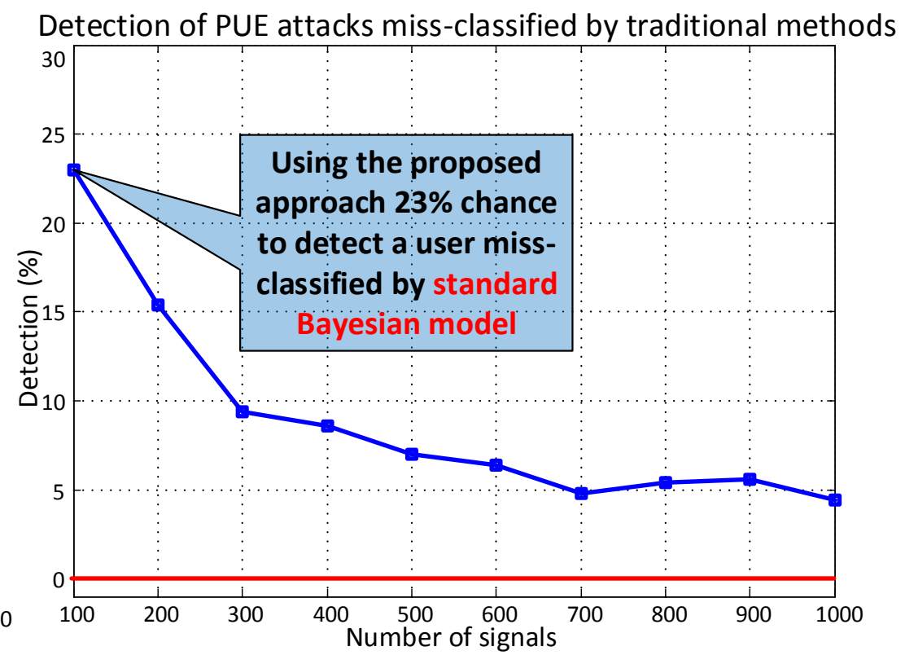
In primary user emulation (PUE) attacks, the attacker generates signals that are similar to a PU to interfere with SUs spectrum sensing process. Fingerprinting, extracting device-specific info. from signals, is used to distinguish real PU from PUE attackers.

The proposed transfer model Use knowledge from past time frames:

1. Extract device-specific information from the environment's signals.
2. Estimate labels:
   - Using nonparametric static Bayesian model.
   - Using abstract knowledge database.
3. Merge results of both the Bayesian model and the proposed model.
4. Update the knowledge database with the final results.



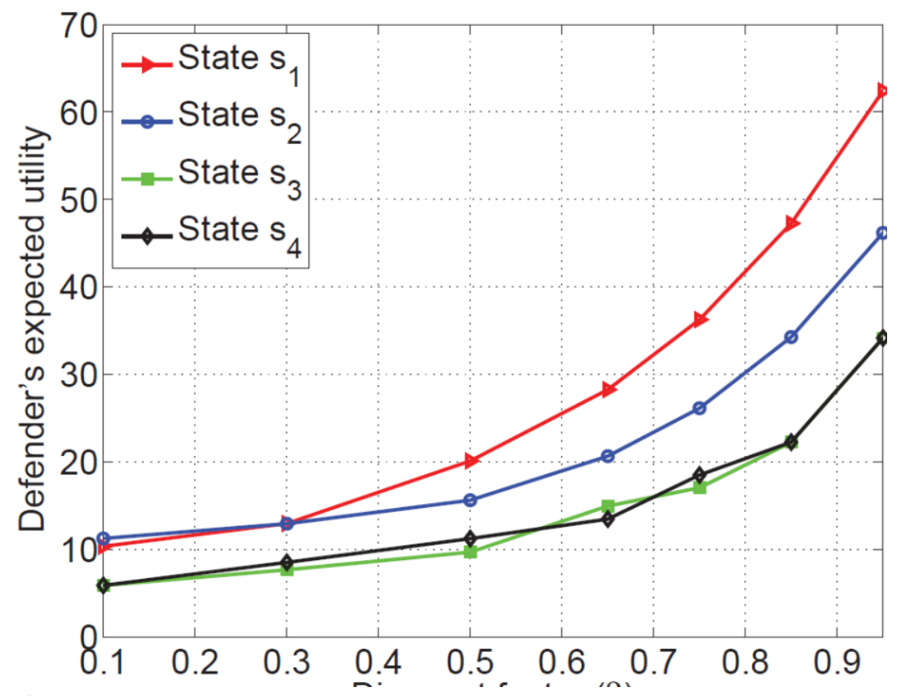

Hit rate comparison with/without the transfer approach

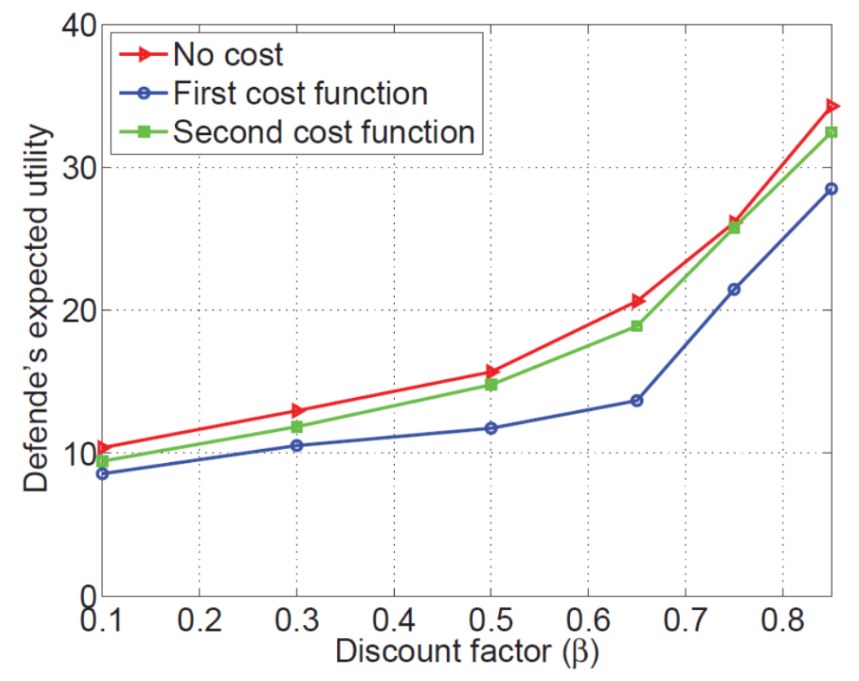

Detection of PUE attacks miss-classified by traditional methods

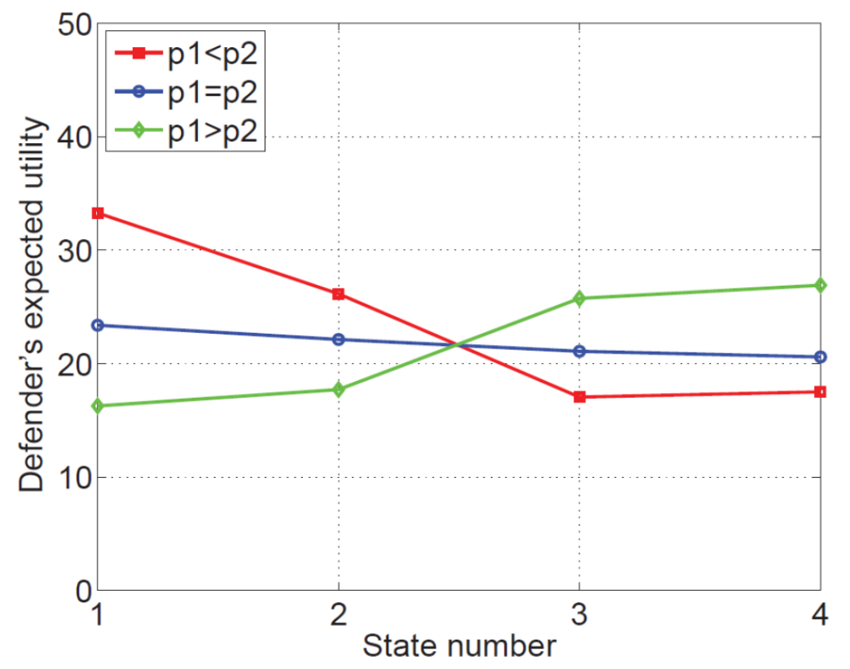
* Y. Sharaf-Dabbagh and W. Saad, "Transfer Learning for Device Fingerprinting with Application to Cognitive Radio Networks," in Proc. of IEEE 26th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Hong Kong, September 2015.

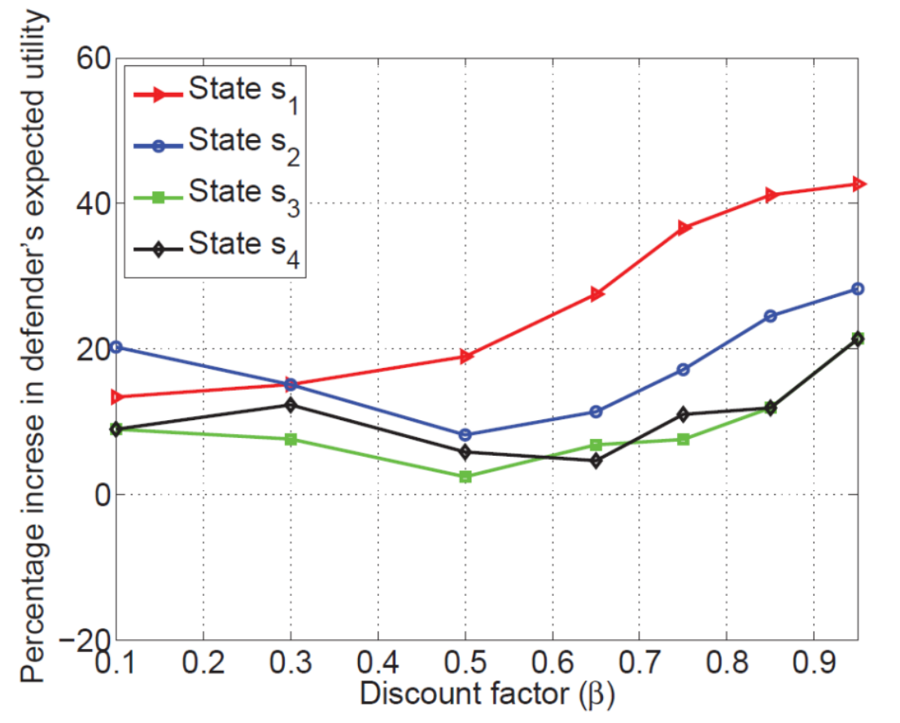
Single Controller Stochastic Games for Optimized Moving Target Defense

- Moving target defense (MTD) techniques that enable a system to randomize its configuration to thwart prospective attacks are an effective security solution for tomorrow's wireless networks.
- The problem is formulated using a non-zero sum stochastic game theory model in which the defender controls state transition.
- The next state is determined only by defender's actions which is suitable for MTD cases where the defender want to change system parameter's before the attacker can reveal them.
- The cost in MTD systems is defined based on the number of consecutive changes in system parameters.









* A. El-Dosouky, W. Saad, and D. Niyato, "Single Controller Stochastic Games for Optimized Moving Target Defense," in Proc. of the IEEE International Conference on Communications (ICC), Communication and Information Systems Symposium, Kualalumpur, Malaysia, May 2016.

On the Authentication of Devices in the Internet of Things

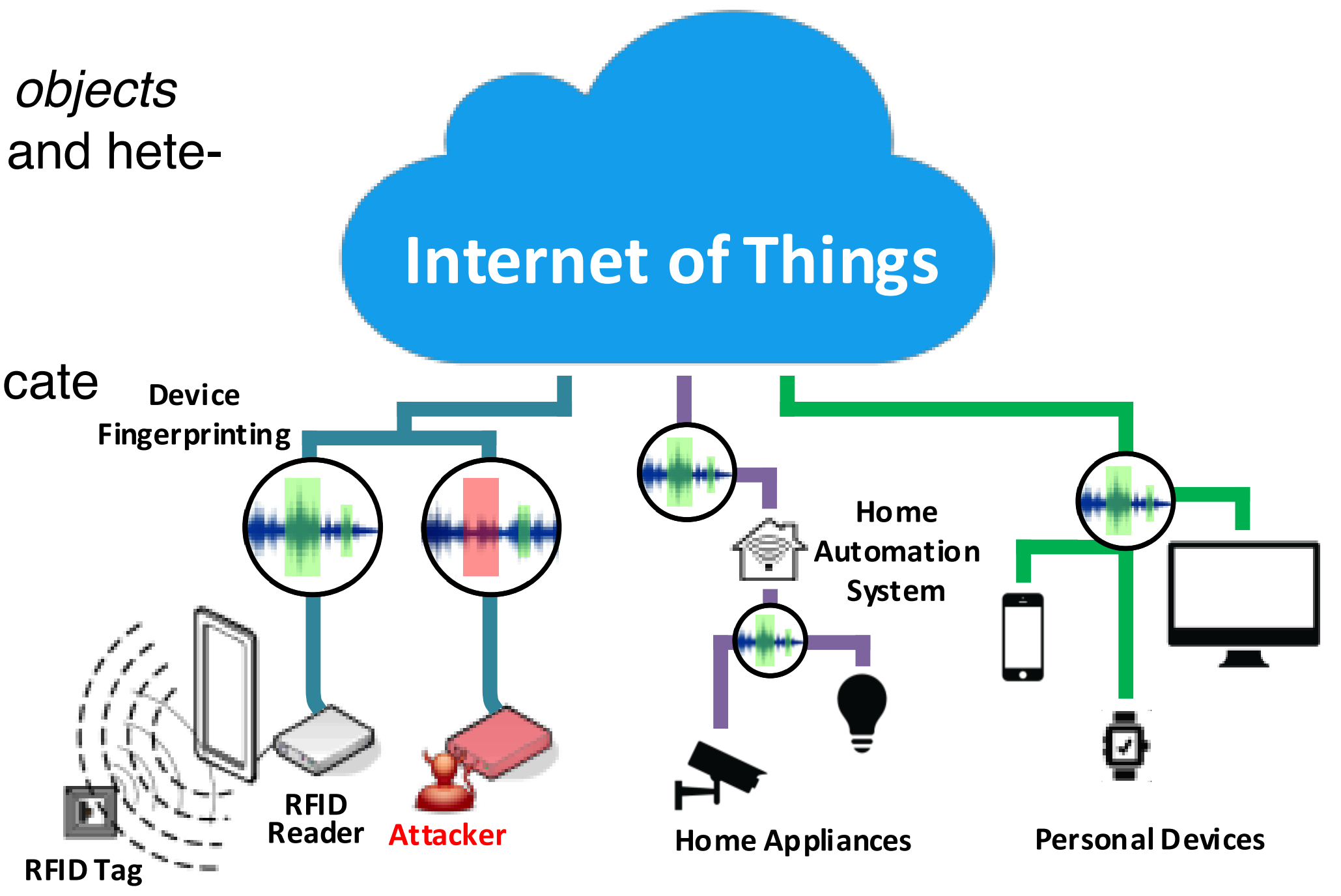
The Internet of things (IoT) is a computing paradigm that allows physical objects to operate over the Internet to collect and exchange data that describes the physical world. To realize the IoT vision, authentication of the interconnections between objects is a fundamental requirement.

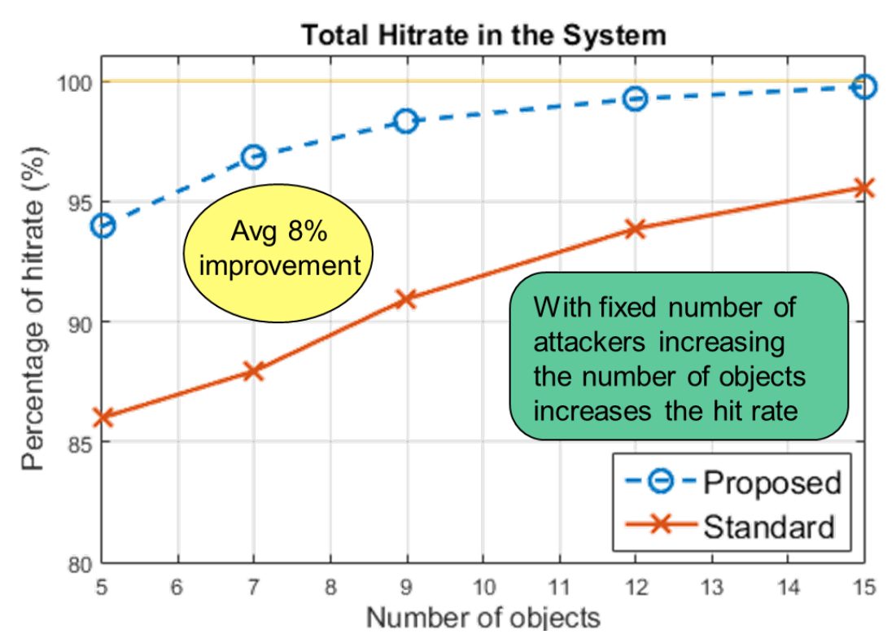
Challenges:

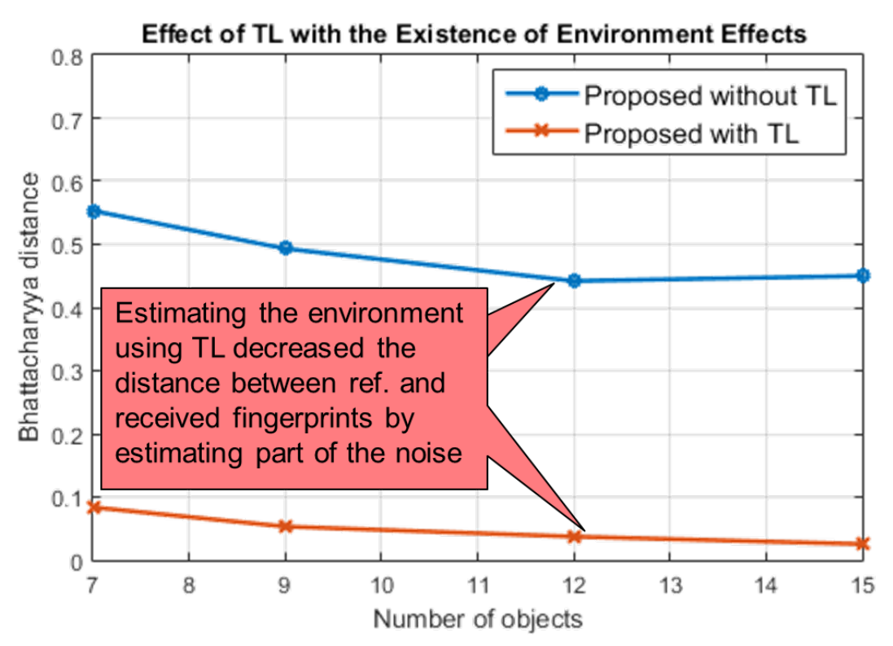
- Most IoT objects have low computation capabilities → *no complex security solutions*
- Some objects only upload data → *no exchange of keys and secrets*
- Plenty of plug and play objects
  → *no preloading of keys on objects*
- Other challenges such as scalability and heterogeneity.

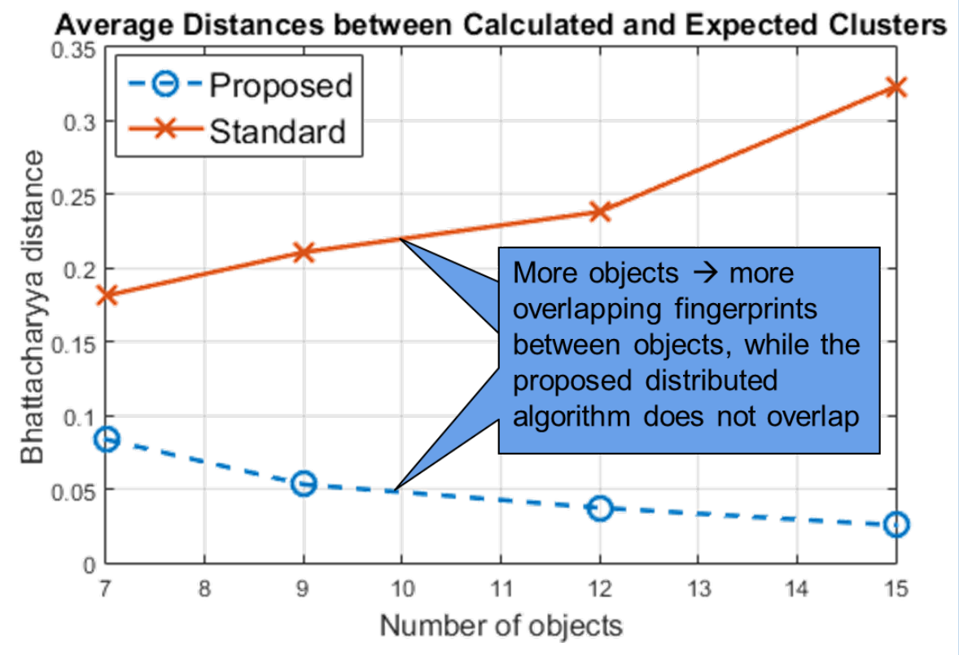
We propose the use of environment-based object fingerprinting to authenticate objects in the IoT.

The proposed framework uses device fingerprinting techniques along with transfer learning to effectively detect emulation attacks




Total Hitrate in the System


Effect of TL with the Existence of Environment Effects

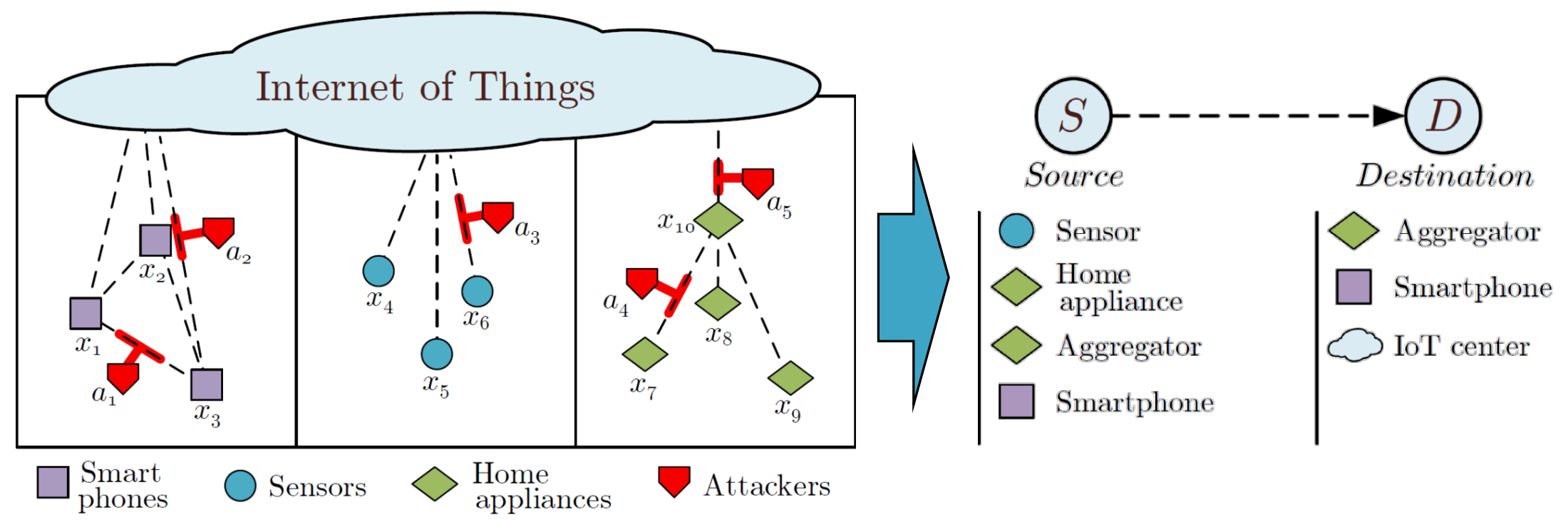

Average Distances between Calculated and Expected Clusters

* Y. Sharaf-Dabbagh and W. Saad, "On the Authentication of Devices in the Internet of Things," in Proc. of 17th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Work in Progress Track, Coimbra, Portugal, June 2016.

Modeling the Internet of Things and Estimation of Environment

In the current work, we model the IoT system as a system with *n* heterogeneous objects, each received message M_S:

$$\underbrace{M_S = F_S}_{\text{Fingerprint of source object}} + \underbrace{w}_{\text{Noise}} + \underbrace{E_S}_{\text{Environment effect}}$$



Probability of detection:

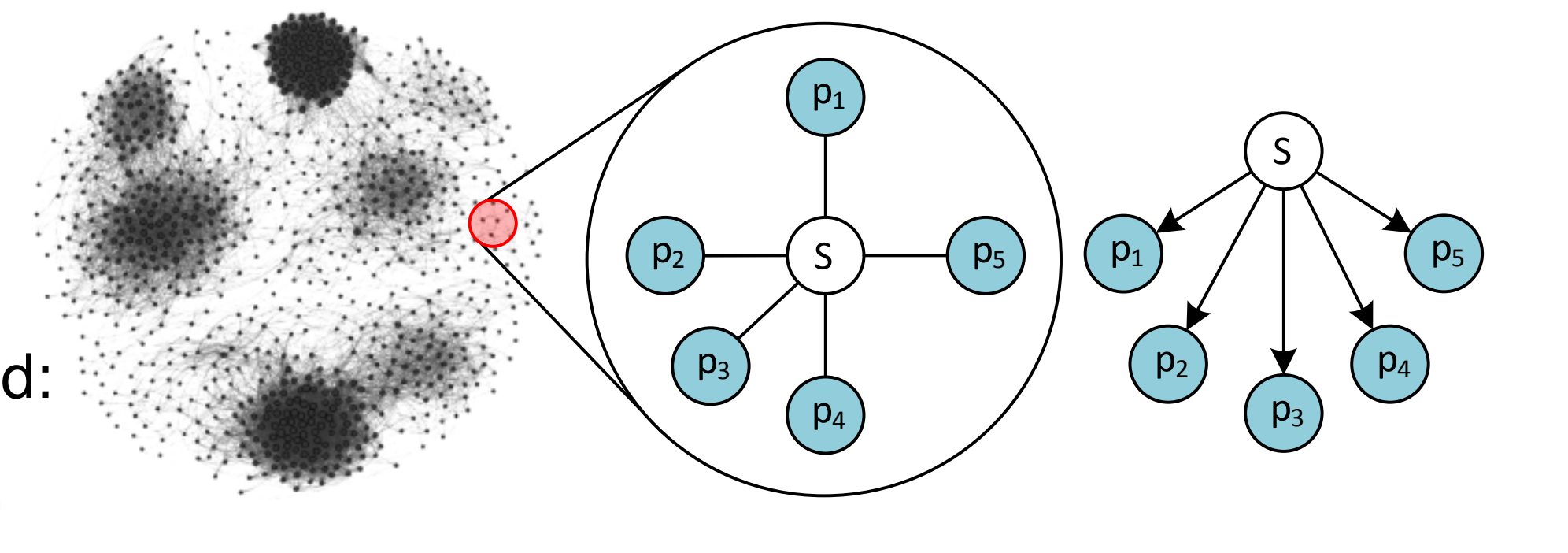
$$P_D = P\{\Delta f > \tau | \mathcal{H}_1\}$$
$$= P\{D_B(f_M, f_M^*) > \tau | \mathcal{H}_1\}$$

Bhattacharyya distance — Distributions of received and reference messages

The environment effect is then estimated:

$$\hat{e}_S = \underset{e}{\operatorname{argmax}} P(e_S = e | P_1, \ldots, P_{np})$$

Estimated environment — Changes in neighboring objects



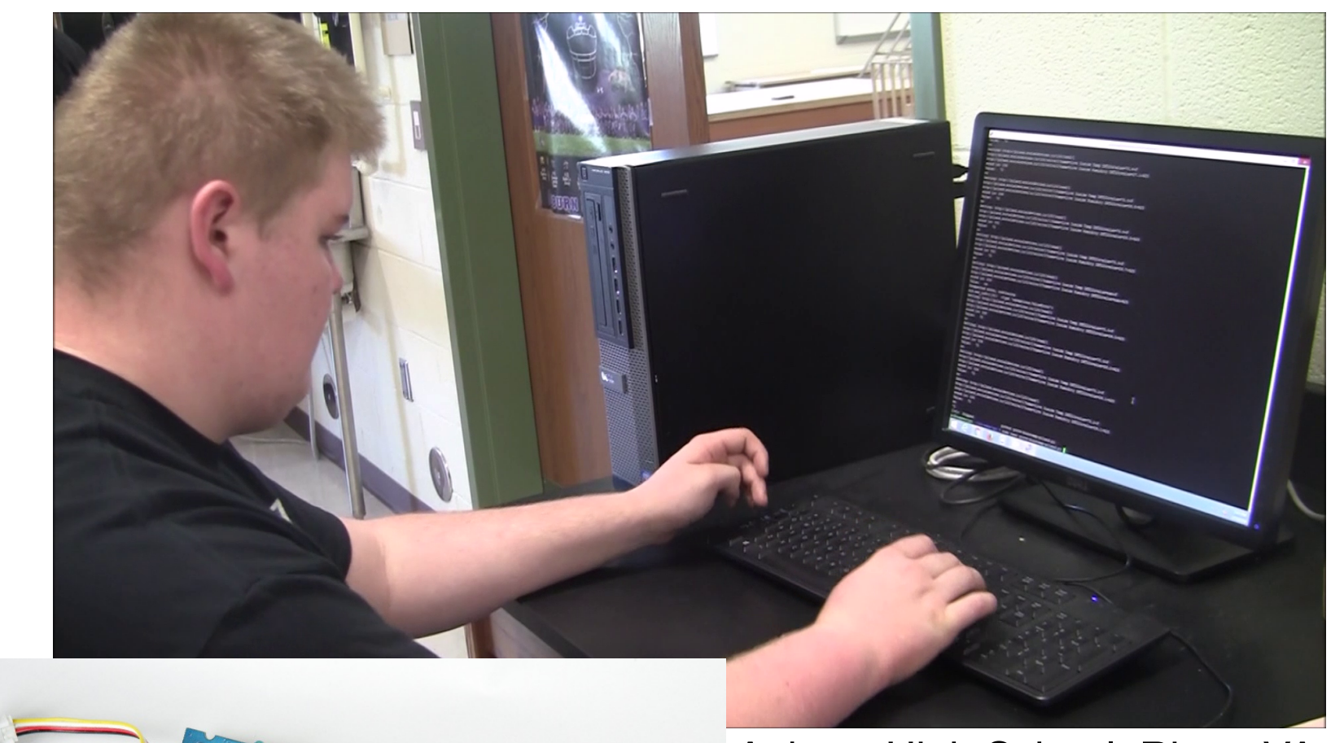
Bayesian network for a set of connected IoT objects

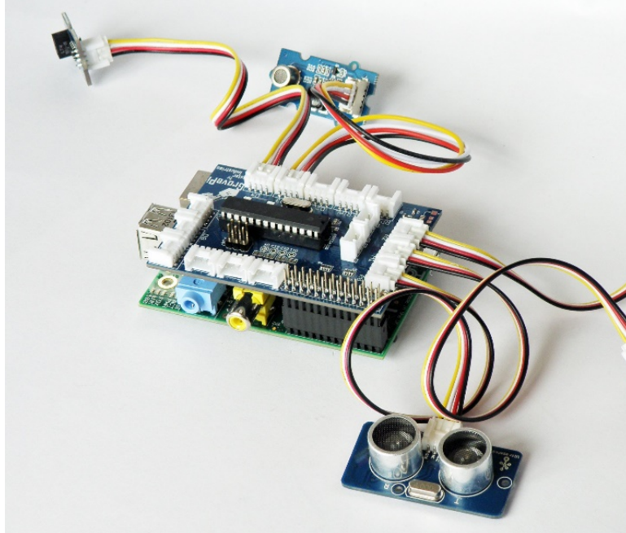
* Y. Sharaf-Dabbagh and W. Saad, "Authentication of Everything in the Internet of Things," on going work.

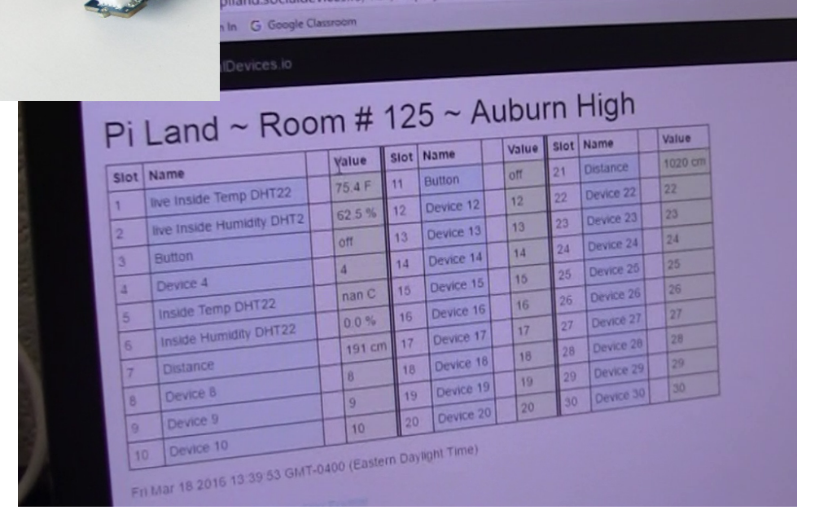
Accelerating IoT Research and Education Under the Global City Teams Challenge and Virginia Tech

The goal of IoT educational project is to bring Internet of Things and smart city concepts to students and future engineers. The IoT project allow students to build a functioning IoT system at school starting from hardware and sensors to IoT data collection center on the cloud.

- Collaborated with the STEM club at Auburn High School to introduce students to IoT environment.
- Participated in a workshop in the C-Tech² program offered by Computers and Technology at Virginia Tech. The program targets rising junior and senior high school girls. Students in workshop implemented small IoT projects starting form configuring the needed hardware, to writing programs, and finally to sending data to cloud.


Auburn High School, Riner, VA

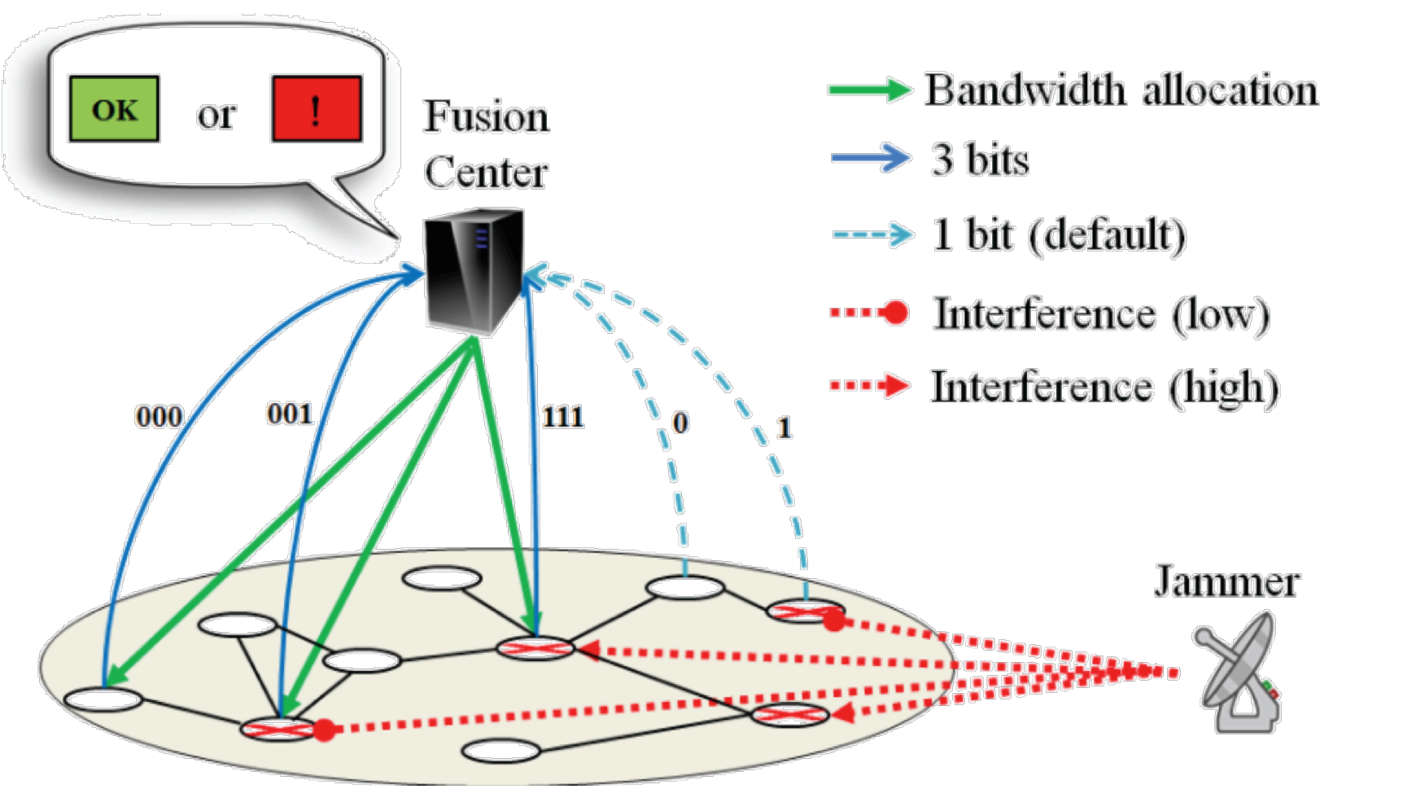

Raspberry Pi + Interface Board

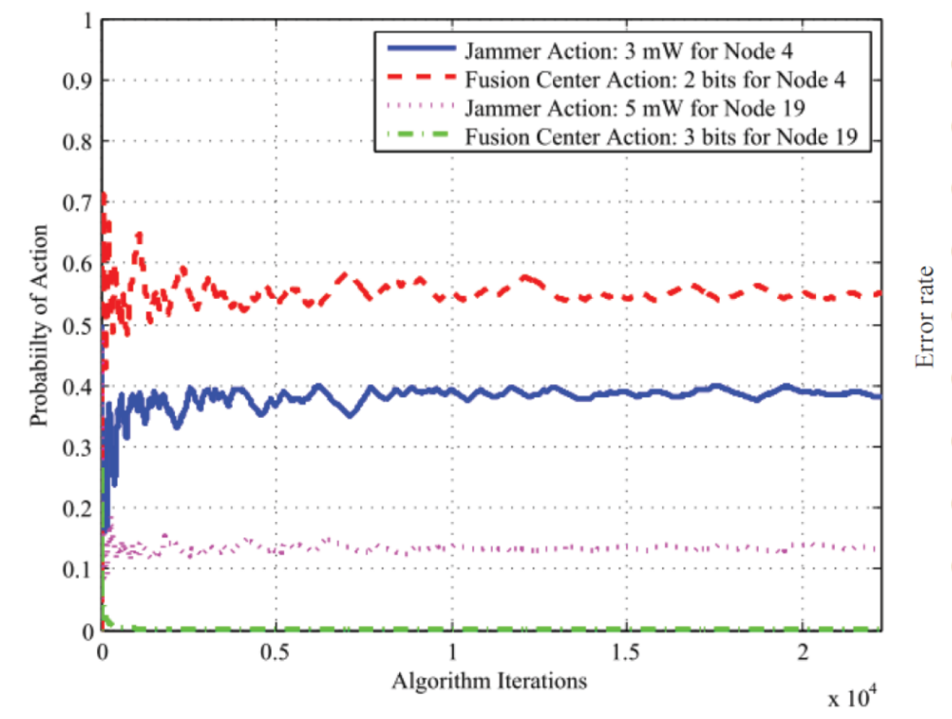


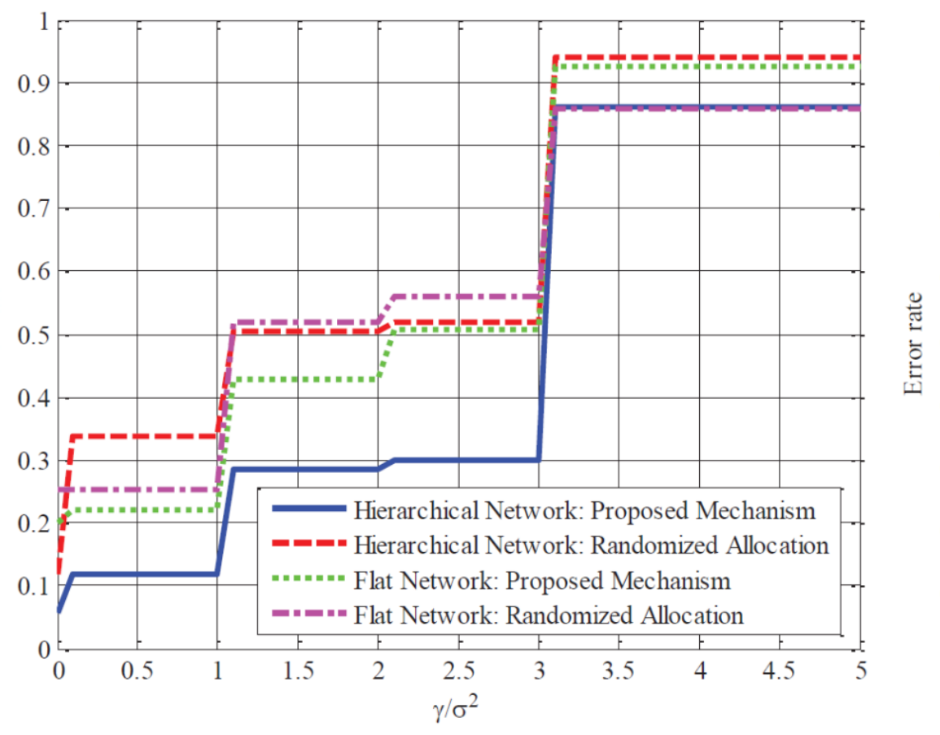
Online data room for Lab125 at Auburn

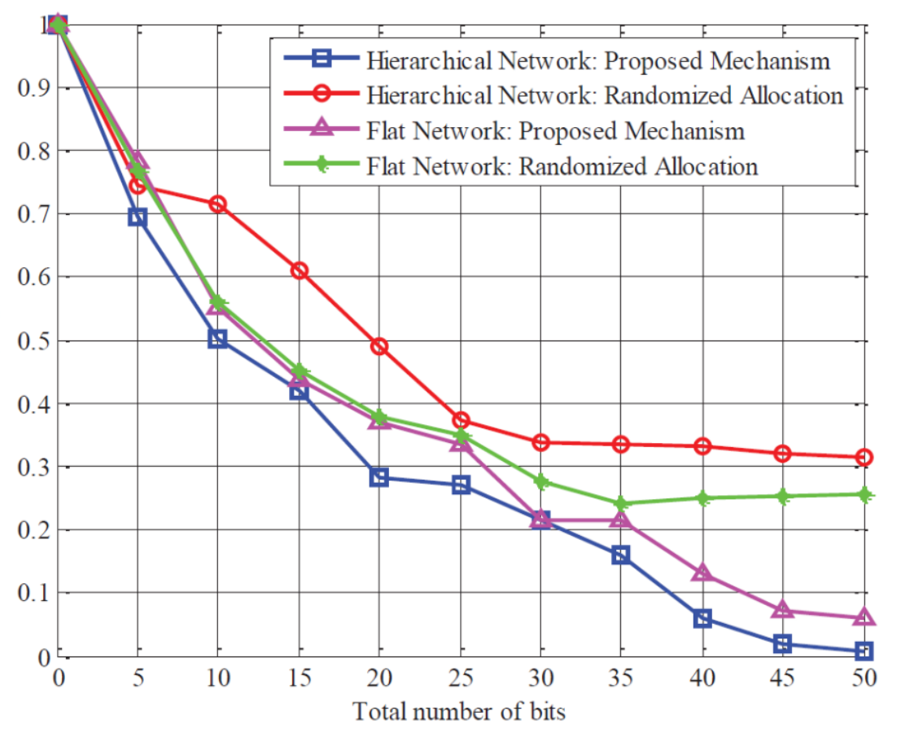
A Colonel Blotto Game for Anti-jamming in the Internet of Things

- Given the heterogeneous and large-scale nature of the IoT, security has emerged as a key challenge. The challenge is further exacerbated by the fact that IoT nodes need to be implemented with low computational complexity. That makes enhancing the security at the physical layer level an attractive solution for IoT networks.
- We model this problem as a Colonel Blotto game and propose a novel anti-jamming defense mechanism against this type of attack using a fusion center.
- In the proposed algorithm, the fusion center was given the opportunity to allocate more bits for certain nodes to improve their interference detection capabilities under the constraint of keeping the total number of bits allocated to all nodes constant.









* M. Labib, S. Ha, W. Saad, and J. Reed, "A Colonel Blotto Game for Anti-jamming in the Internet of Things," in Proc. of the IEEE Global Communications Conference (GLOBECOM), Communication and Information System Security Symposium, San Diego, CA, USA, December 2015