Paul M. Washburn

CSCI E-11 Unit 2: IoT

November 2, 2019

**Future Technology: Office Networking App – IoT**

Several technologies from the IoT unit could be combined in the development of an Office Networking App. Unlike many industrial applications of IoT technologies – which are typically straightforward collections of data streams relevant to some production process – this use-case requires creative applications of IoT to help deliver value to professional users like Dr. Brown.

One application IoT is the use of low-cost microphones to collect a verbalized journal entry of each user that describes their professional interactions for the day. This data can be mined for patterns by the Office Networking App. Most of these microphones could be networked from existing applications, such as a self-driving vehicle, so that users like Dr. Brown do not need to be at a specific place in order to dictate their diary entry for the workday. This greatly decreases the need for establishing an entirely new infrastructure of microphones to collect the data. Dr. Brown’s location when he records his dictated journal entry will dictate what type of process will be used to record & process the data. When he is in a self-driving vehicle, on-board microphones will be plugged into the car’s main computer system and thus will not have battery concerns, and neither data volume-per-day nor device-to-gateway range will be a concern since the vehicle can be used as a “data mule” and transmit data when connected to WiFi at night time. Microphones will need to be installed in his office to allow for times when Dr. Brown is dictating his thoughts about his daily professional interactions when he is physically in the office. By installing a few microphones in his office that are directly connected to power, Dr. Brown can choose whether to dictate his thoughts in office or during his ride home – both of which are private environments. If the entry is recorded in the office then the office WiFi can be used to transmit data to the cloud; otherwise the community self-driving vehicle will prompt a data dump when it is idle and connected to WiFi for the day. Device-Cloud-Device is the architecture of choice for this app.

Indoor localization techniques combined with inexpensive indoor temperature sensors will be leveraged in this application to ensure Dr. Brown and his colleagues are never too-hot or too-cold in a meeting again. Integrating temperature preference data for each user with meeting attendance data from the Virtual Assistant will inform the Local Warming technology which users are comfortable at which temperatures. Users like Dr. Brown will be able to initialize their desired temperatures as a starting point, but over time the system will use wireless reflections of the human body to identify if a given individual has goosebumps (indicating they are cold at the current temperature setting) or if they are sweating (indicating they are hot at the current temperature setting). If a too-hot or too-cold flag is raised during a meeting, then at the end of the day the Office Networking App can ask Dr. Brown a quick *“Were you too hot/cold during your noon meeting today?”* to provide feedback into Dr. Brown’s preferences. By being cognizant of users’ temperature preferences we can ensure that all of the professionals using the application will always be physically comfortable during meetings – and being too hot or cold will never prevent them from contributing in a meeting.

The above indoor localization techniques could also be combined with camera data & wearable data to direct the lighting in a given meeting room at exhibitions focused upon by the speaker’s inferred angle of gaze. While highlighting the object of Dr. Brown’s presentation, this system will also help Dr. Brown’s audience take notes by shining lighting directly on their notebooks. When a given member of the audience is not taking notes, their lights will shut off to save on energy.

The microphones and cameras installed in meeting rooms will also be used to identify and surface tense interactions between colleagues, effectively identifying negative outliers in the “productivity” of a professional interaction. This will be especially useful in large meetings where interactions between colleagues are rapid-fire and pass by quickly. Voice recognition, speech to text, sentiment analysis, facial recognition & micro-expression classification (among other machine learning techniques) can be applied to the data collected in order to identify such “tense” interactions. Furthermore, indoor localization techniques similar to those described above could also be used to measure breathing and heart rates to identify large jumps in heartrate and/or breath. Since this is an example of outlier detection, much of the “non-tense” raw data will not be of much interest. In the spirit of keeping just the data we need we would likely discard the raw content of the benign/neutral interactions, but keep the metadata and outputs of the summarization processes for these records. For interactions that were sufficiently “tense” all of the raw data (e.g. audio/video, text translation) will be kept alongside the summarization process to allow for deeper analysis. While hopefully the vast majority of interactions that Dr. Brown has with his professional colleagues are not “tense”, this feature will be able to notify him when it occurs – and recommend some actions to help mitigate the damage & improve the relationship.

WEARABLES AND SENSORS TO DIRECT LIGHT TO WHERE TO LOOK

**IoT** Outline

* 7.1 Network Connectivity for IoT
  + IoT network design space; GB per day, device-to-gateway range, battery life
    - What space we’ll occupy and why
* 7.2
  + How are we dealing with
    - Limited resources
    - Missing/noisy data
    - Outliers/anomalies
  + Continuous, real-time recognition
    - Detection-feature extraction-classification
  + Where is BLE low power stuff relevant
  + Strategy for collecting only data we need: Energy and Bandwidth restrict the amount of data we can collect
    - Battery life vs. quantity of data; latency vs. resolution
    - On-device processing, tradeoffs
    - WiFi/Bluetooth use MUCH less energy than 3G/LTE
    - How can data be combined as it is transmitted through the network?
    - Intermittent/low-rate radios limit what can be collected
      * Considerations
        + Continuous Monitoring vs. Alerting
        + Buffering to mitigate rate variations & dysconnectivity
    - End-to-end principle: Data should only be removed from a device when it has been delivered to permanent storage
  + IoT data is approximate: It arrives at discrete times, Data is of limited precision, Data can even be wrong
    - Interpolation; extrapolation (regression);
    - Smoothing; curve-fitting, low-pass filters
    - Alignment; auto-correlation, dynamic time warping
    - Technology usage: FunctionDB to allow users to fit continuous functions to raw data
  + Anomaly Detection: Automatically flag outliers. Identify common properties of outliers. Rank & triage outlier classes.
    - Detect anomalies via an Anomaly Detector (e.g. human labeling, robust statistics)
    - Detector feeds both an Inlier Classifier (frequent itemsets) and an Outlier classifier (frequent itemsets out of all the infrequent itemsets)
      * Feed a ranking algorithm (Mahalanobis distance)
  + Anomaly Explanation: We’ll need to tell people what the fuck is up
    - Use classifiers (e.g. decision trees, SVMs, frequent itemsets)
    - Frequent itemsets works for categorical or binned continuous variable data
    - “Given an outlier group, find a predicate over the inputs that makes the output NO LONGER an outlier”
* 7.3 Localization – nothing relevant from this module
* 8.1 Protection from Ransomware – prevent attack on the service & infrastructure
  + Security is a negative goal
  + Prevent:
    - Changes to permissions to access files fraudulently
    - Direct disk block access
    - Internet access
    - Reuse of memory
    - Accessing backups
    - Interception of network packets
    - Trojan text editors
    - Stealing disk of server(s)
    - Spoofing sysadmin – personal knowledge
  + Threat model:
    - Adversary controls some computers/networks but not all
    - Adversary controls some software on computers he controls, but not full control
    - Adversary knows some info, such as passwords or keys, but not all
    - Adversary knows about bugs in software
    - Physical attacks?
  + How we’re assuring unrealistic threat models
  + How disabling a holistic view of the system might work
    - Prevention: increase difficulty of attacks
    - Resilience: allow system to remain functional
    - Detection/Recovery: allow systems to quickly detect & recover from attacks to a fully functional state
  + Physical Unclonable Functions PUFs for enabling secure, low-cost authentication
  + Shrinking the Trusted Computing Base
  + Tamper-resistant hardware to prevent private information stored on the hardware
    - Ascend Processor for IoT to eliminate leakage over chip pins
* 8.2 Human Computer Interaction
  + Designing an interface that is User-centric
    - Use speech-to-text to avoid typing
    - Speech – understanding – dialogue – generation
  + Reasons for speech applied to information access & management:
    - Information space is broad and complex
    - Users are technically naïve
    - Device is small
* 8.3 Robotics & Autonomous Vehicles
  + Concept of “Google for the physical world”
    - Extend analogy to building a topology of professional relationships
    - What and who are where? Maintain as a function of time
  + SLAM – Simultaneous Localization And Mapping – is likely not useful here
* 9.1 Smart Buildings
  + Sensate materials: measure temperature & decibel level of meetings and work environments – automatically adjust environment to preferences
* 9.2 Smart Homes
  + Use indoor localization to identify when people who rarely come in are present; prompt fruitful connections between others
    - Multipath effect can be exploited to increase accuracy: spatial angle profile of the power reflected
    - Combine this with badges used to scan into different parts of buildings
    - Breathing & heartrate could be measured during meetings in conference rooms to determine “stress levels” when person A interacts with person B
* 9.3 Smart Cities
  + Number of connections between colleagues might help inform seating/office charts similar to mapping telephone calls
  + Local Warming type technology could be deployed to ensure users are operating at their “optimal temperature” during meetings
* 9.4 Conclusions
  + How will component technologies (location, sensors, interfaces, setup, robotics, vehicles) interact with the system design (networking, architecture, data management, security)
  + Device-Cloud-Device will be the architecture of choice since real-time data is not always required
    - This won’t be true for real-time tracking of people in the office
    - Things will be lifted to the cloud and use internet protocol & web standards; use local controller/gateway for performance