CSCI 5273 - Paper Review #2
Kevin Hallock
2020-11-13

Paper information:
Title: Rethinking Wireless Network Management Through Sensor-driven Contextual Analysis
Authors: Shazal Irshad, Eric Rozner, Apurv Bhartia, Bo Chen
Publish date: March 2020
URL: http://ericrozner.com/papers/HotMobile2020.pdf

Paper Summary:

This paper proposes a theoretical network architecture called “SenseNet”. As presented, the SenseNet architecture would combine the use of “out-of-band” sensors (particularly video cameras), deep/machine learning algorithms, and “edge computing” clusters (powerful servers co-located with the network access point) to enhance Quality-of-Service (QoS) for client devices on a wireless network. In this context, “Out-of-band” information refers to information about an environment pertaining to clients that is acquired through means outside of the existing network infrastructure, such as video cameras, proximity sensors, or other environmental sensors; this information is explicitly *not* obtained through the existing network infrastructure. Conversely, “in-band” refers to information obtained exclusively through network equipment, such as signal strength or round-trip time.

Essentially, there are three components to the SenseNet architecture: collecting data using out-of-band sensors, analyzing the data using machine learning techniques on powerful “edge computing” clusters, and then applying network policies to users on the wireless network based on the result of analyzing the data.

The authors suggest the use of cameras due to an extensive network of video cameras being used for surveillance or other CCTV purposes already existing. The authors also acknowledge that advanced deep/machine learning algorithms that can classify/categorize images/video already exist, and that this technology could be used to analyze the data collected by the cameras. Finally, the authors propose following a common industry trend of using powerful computers co-located with the network access point equipment to perform the analysis.

The paper describes numerous use cases in which the SenseNet technology could be utilized for societal good, such as using cameras to identify people with injuries in some sort of emergency scenario and providing them with better Quality-of-Service on the network in order to contact someone for help. Another idea is that network services could be denied to someone who is deemed to be an intruder. These ideas both depend on out-of-band information that cannot be gleaned simply from a device fingerprint or network usage patterns.

The authors provide a simple real-world example of how out-of-band data camera data can be translated into something meaningful such as “blue shirt” or “green truck” with machine learning.

They offer a vision for how network devices associated with an identified characteristic can be assigned a network performance policy; an example of this would be that perhaps wireless users in hybrid or electric vehicles could be given higher network priority than wireless clients in a large truck as a sort of incentive to using greener technology.

After offering example use cases, the authors then demonstrate a proof of concept experiment that uses a single camera and three wireless access points. The access points are used to triangulate a wireless client's location based on the device's latency to each access point, and the camera is used to locate the device's position in a visible-physical domain. By matching up the device coordinates with an individual's location, network policies can be applied on a per-user basis, rather than per-device.

Strengths:

- This paper proposes a novel use of existing technology (cameras, deep learning, edge computing) for enhancing network performance and Quality-of-Service. Using commonly deployed devices like cameras makes it easy to expand the network, the biggest cost is in the necessary computational power.
- The authors suggest several compelling real-world use cases that would benefit from this technology, which help paint a clear picture for how this technology should be investigated further.
- Several ideas for monetizing SenseNet technology are proposed, particularly for marketing purposes. I am personally not a fan of this technology being used for advertising, but I believe that this is a strong proposal if the purpose of this paper is to seek additional funding and collaboration.

Weaknesses:

- The required computational power needed to perform the necessary data analysis is infeasible for deployment on a wide scale; I think the technology would ultimately be more feasible if implemented on a room- or building-scale infrastructure.
- Network security is a difficult enough challenge, but I fear that it would be even easier to spoof real-world things like shirt color, etc in order to trick an out-of-band sensor.

What I learned from this paper:

Prior to reading this paper, I had never considered the idea of using cameras or other out-of-band sensors to enhance network performance or Quality-of-Service. This is a fascinating area of study and I'm intrigued to learn more about possible uses of out-of-band information for network optimization.

While unrelated to the content of the paper itself, I learned what a "position paper" is. After the very formal nature of the paper I reviewed for my first paper review, I anticipated that this paper would detail a similarly complete project; however, it seems that the SenseNet architecture is in

the earliest stages and that the purpose of this paper is to enable discussion around the emerging combination of technologies, as well as to solicit possible collaboration and/or funding.

What are the avenues for future work that you think are important? If you are asked to work on the problem studied in this paper, what will you do differently?

The authors explicitly identify this paper as a “position paper”, meaning they’re proposing an idea that could be worth further investigation, and I strongly agree that this topic is worth exploring further. In particular, none of the deep/machine learning techniques that were proposed to be used with the out-of-band camera data was actually used in the authors’ current methods; I feel that integrating all of the proposed pieces -- machine learning, matching triangulated wireless locations with physical locations in a camera image, assigning QoS policies -- into a full implementation would be an excellent next step in demonstrating the usefulness of SenseNet.

The authors mention that the camera location identification becomes less effective near the edge of the camera’s field of view and that a combined WiFi-and-camera localization technique is helpful for narrowing down a client’s location in this case. They specifically want to come up with a scheme for weighting the WiFi and camera data to improve the localization accuracy.

Finally, I am curious what would happen if multiple cameras were used to improve the localization of clients in the visual-physical domain. Because of the shortcomings of localizing a point near a single camera’s field of view, this seems like a promising way of improving the accuracy of the camera’s localization. Additionally, if SenseNet were to be implemented using CCTV systems in a city for example, then there would almost certainly be multiple cameras covering a given area, so investigating the use of multiple cameras would more closely mimic an eventual real world use case.

Detailed comments:

I was particularly intrigued by the idea of using SenseNet to associate multiple wireless devices with a single user and then grouping them under a single Quality-of-Service policy for a network. Assigning multiple devices to a single user using existing technology can only really be done if the network administrator knows about all devices in advance and can associate them with an individual.

Although the technology seems like a promising field of study, I am very concerned about the privacy implications of using it on a large scale. I recognize that users can generally already be identified on a network, but to identify an individual’s clothing or appearance and use that to restrict or prioritize access to a network seems like a slippery slope, and I believe that it would be essential for there to be regulations in place to prevent corporations or political entities from abusing the technology.