Sensor Network Virtualization for Cloud-based Remote Sensing

Tingzhi Li, Marco Falke, and Jinming Mu

***Abstract*—In real world, the actual network infrastructure can be dynamic. With the help of network virtualization, we are able to performan remote sensing task regardless of physicial network changes. For a given network, if we tried to perform any task, the first crucial step is be able to spread the task requirement in the network in an effecient manner. In short, task message need to be broadcasted quickly. In this paper, we used ns-3 to implement gossip protocol.**

The abstract goes here.

***Index Terms*—IEEEtran, journal, LaTeX, paper, template.**

I. Introduction

Smartphone, smartwatch, and smart thermostats could form a network in which these devices could communicate with each other. If these devices are connected to the Internet, we call it the Internet of Things. There is no doubt that IoT is an innovative paradigm [1] because this idea combined the Internet with our everyday gadgets. Either from the perspective of private user or from the perspective of business user, there are infinite possible ways to exploit IoT. As of today, research in the area of IoT is emerging rapidly and many open questions remain to be answered.

Remote sensing is one of the possible services of IoT. Remote sensing involves the search and selection of IoT devices to form a virtual sensor network. Subsequently, the selected devices estimate the wanted property collaboratively and report the result to the remote cloud agent. IoT assigns a unique MAC address to physical object which do not have an identification, so people could track the specific objects status and control it remotely. The advantage of remote control is that it requires less manpower needed to monitor and manage the object. And it could further increase devices usage rate. However, the main challenge here is that IoT devices are often resource limited meaning they have limited bandwidth and power, and restricted by their mobility. Due to the characteristics of IoT devices, topology of physical network formed from IoT is dynamic. The distributed network protocol which virtualizing the physical network has to deal with this dynamic nature of IoT networks. Therefore, it is important to evaluate the distributed network protocols performance under various power models and different MAC protocols in ns-3.

This demo file is intended to serve as a "starter file" for IEEE journal papers produced under LaTeX using IEEEtran.cls version 1.8a and later. I wish you the best of success.

mds

September 17, 2014

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here:

Subsubsection text here.

II. Problem Statement

Our project goal is to evaluate the performance of a virtual network protocol consisting of IoT devices in ns-3. The major step here is that we will first simulate a wired mesh network with a given topology file. Then we will replace the wired Ethernet mesh network with wireless mesh network. Based on the new wireless mesh network, we will plug in models representing IoT devices characters and implementing protocol to evaluate its performance.

A. Network scenario 1: Wired Network

In this network scenario, we will try to simulate a wired mesh network with a given topology file. But first, a simple peer-to-peer network formed of nodes connected by a 100 Mbit/s Ethernet connections is looked onto. And then we will elaborate this peer-to-peer network to a wired mesh network with a certain topology. That topology is defined by a file that contains the information about the nodes and edges of the network.

B. Network scenario 2: Wireless Network

Based on the wired mesh network, now we could replace that with a wireless mesh network. The topology is the same as the wired mesh network. Depending on different wireless technologies, we could define different connection rate. For example, zigbee and 6lowpan has the same maximum speed of 250Kbps. But WiFi Direct connection speed could be up to 250Mbps. Then we could plug in random variables representing random locations of devices, random packet drops of the network and power consumption of devices. Finally, we could implement the protocol to evaluate its performance.

III. Related Work

In this section, we introduced the topic of Virtual Networks formed using a subset of a large group of IoT devices. Relevant papers covering the topic of Virtual Networks are summarized. In addition, one paper about WiFi Direct technology is summarized as well.

A. Virtual Networks

The following sections will present an overview over Virtual Sensor Networks, as well as network virtualization using the existing internet.

1) Virtual Sensor Networks: The ongoing technological progress further and further improves the computation, connectivity and sensing capabilities of various devices, sometimes mobile ones. [2]This enables a huge variety of opportunities in sensor networks. For example, devices in a sensor network could be assigned tasks based on their constraints in computation, power usage or networking potential. In contrast to dedicated sensor networks, where the participating nodes serve a single application, Virtual Sensor Networks (VSN) take advantage of the nodes technological progress. When a VSN is formed on top of a Wireless Sensor Network, only a subset of all available nodes is part in the VSN. Furthermore, several VSNs can exist simultaneously in on Wireless Sensor Network. [2] That is, one subset of the nodes forms a VSN and relies on the remaining nodes to communicate between its nodes. In some cases, physical nodes of one VSN even could be completely cut off from communication due to their spatial distribution and must rely on the other nodes. Usually the different VSNs pursue completely unrelated sensing tasks and the nodes in each VSN behave like they are on their independent Sensor Network. Figure 1 based on [2] depicts a visualization of twoVSNs formed on top of an Wireless Sensor Network. This logical separation helps to simplify the implementation of applications significantly. [2] Further advantages of VSNs are enhanced performance and better scalability. The development of algorithms and protocols to support the grouping of VSNs on top of Sensor Networks, is still an ongoing research topic. Those need to consider how the available time and frequencies should be fairly distributed for intra network communication. Moreover, it should be possible for nodes to change their membership in VSNs.

2) Virtual Networks on Top of the Internet: It is important to realize that the Internet, due to so many different participants with sometimes opposing interests, is hard to modify and only possible small and slow steps, if at all. Therefore, Virtual Networks are often the only way to realize innovation. To implement a Virtual Network using the existing Internet, several things need to be considered. First, the characteristics of the networking technology determine the attributes of the Virtual Network. For instance, a wired network yields a more scalable and bandwidth flexible Virtual Network than a wireless network would do. [3] Second, the layer of virtualization (referring to the OSI layer model) impacts the flexibility of the Virtual Network. That is, the lower the layer of virtualization, the more flexibility will be possible. Specifically, so called overlay networks, mostly realized in the application layer, are limited in their ability to support fundamentally different architectures. [3] Moreover, virtualization on top of IP is fixed to the network layer protocol and can not deploy IP independent mechanisms. [3] Lastly, an important consideration in the non comprehensive list is also about security and privacy in virtual networks. Thus, attack vectors such as denial-of-service or distributed denial-of-service against the underlying physical network will have impact on all simultaneously virtualized networks.

3) Virtualization Algorithm: Though, it is possible to form a VSN of mobile IoT devices by having access to all relevant data such as availability, sensor capabilities or sensor mobility, a more efficient solution is to assume the managing cloud agent does not have full knowledge of every sensors properties. [4] The cloud agent even may not be connected to all nodes but only to a subgroup of them. The presented algorithm also takes into account mobility of the devices which sometimes leads to nodes being unavailable for some time. [4] This virtualization algorithm will search and select appropriate sensors from the whole network to form the virtual network which then executes the sensing task.

B. WiFi Direct

WiFi Direct is a technology that its goal is to improve direct device to device communications in Wi-Fi [5]. The main strength of this technology is that it doesnt require the presence of an Access Point [5]. Actually direct device to device connection was already possible by the ad-hoc mode. But it is not popular because the ad-hoc mode is not power efficient [5]. Instead WiFi Direct uses WiFi infrastructure mode [5]. It let devices negotiate who will be the AP in this network [5]. By doing so, it obtains all the enhanced QoS, power saving, and security mechanisms originally developed for the WiFi infrastructure mode [5]. After first establish the network, new devices could connect to this network just like connecting to an AP [5].

IV. Solution

V. Conclusion

The conclusion goes here.

Appendix A
Proof of the First Zonklar Equation

Appendix one text goes here.

Appendix B

Appendix two text goes here.

Acknowledgment

We would like to thank Dr. Bechir Hamdaoui for his advising. We also would like to thank Sherif Abelwahab for his advising.

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

Michael Shell Biography text here.

John Doe Biography text here.

Jane Doe Biography text here.