

ECE1776: Project Midterm Update - Kiran Gollu(994392787)
Worm Detection and Eradication in Bluetooth Environments

Our initial goal for the final project is to develop a model for analyzing and modeling human encounters. Our next goals are to incorporate this analysis into worm propagation model and investigate blue tooth worm prevention. As a part of blue tooth prevention, different inoculation policies/quarantine policies(who to inoculate/quarantine/rescue) will be studied and finally, the most effective method will be presented.

Our methodology here is study a simpler problem: analyzing human encounters as opposed to human mobility patterns. Person's encounters describe **when** and **who** they meet without specifying **where** the encounter occurred. While losing geographical information, studying encounters helps us to understand how information propagates in the context of new, mobile Internet systems.

An encounters model would be useful in many applications that appear to require a mobility model. For example, encounters drive the workloads of the Bluetooth-dating application(<http://www.proxidating.com/>). Furthermore, gathering encounter data in order to validate the model is much easier than gathering an equivalent amount of mobility data. For applications where encounter-modeling is sufficient, our model should be able to present much more believable results, since it can be more thoroughly validated against real data.

Our initial results and previous work have the following implications on Internet systems for small devices:

- 1) System load is predictable
Driven by time of the day and day of the hour
- 2) System load is highly unbalanced
Long tailed distribution of encounters
- 3) Caching is likely to be effective
Most time is spent meeting friends though people meet strangers often.

The problems described comes down to solving following three problems. The status of the project in relation to three problems is presented below.

Global Popularity Graph: How many encounters does an individual make with others? And with whom? This requires determining the contact sets for each individual which contains the list of individual he encounters.

Inter Encounter Graph: How does the inter encounter time distribution look like for the entire population? And per individual? We are in the process of developing a model for the same. We are also trying to figure it's correlation with the global popularity model.

Duration of encounters: what is the approximate duration of these encounters? We haven't made any progress on this so far.

We are currently verifying our global popularity model and inter encounter against the five different mobile traces MIT reality mining trace, Hagggle trace1/2/3, and NUS trace. Our methodology here is to study the above three characteristics on these traces and prove that our model produces believable results for human encounters.

Project Status:

What is done?

Global popularity graph is almost finalized. Andrew developed a method that generates contact sets for each individual in the population. Currently he is working on the inter encounter distribution problem. I have verified the results of the global popularity graph with four traces from Dartmouth college. Inter encounter graphs are being studied for the four traces. Also, we are looking at the encounter sharing graphs as well.

What needs to be done?

- 1) Develop a model to understand inter encounter time distribution. Our claim here is that it follows an exponential distribution with a per-hour average.
- 2) Verify inter encounter time distribution model with the four CRAWDAD traces.
- 3) Study blue tooth worm prevention techniques using our model:
 - Analysis on worm infections can spread over blue tooth environment?
 - How quickly a particular device can infect X % of the population
 - Study different to inoculate devices to ensure minimal infection for the population (like inoculate only top 10 popular guys in the population etc.)
 - Study different quarantine policies (e.g. put a monitor to identify infected devices and quarantine them etc.)
 - Would a proactive reboot slow down a worm massively?
 - what is the most effective method?

Sources for CRAWDAD Traces:

MIT Reality Mining Trace

<http://crowdad.cs.dartmouth.edu/meta.php?name=mit/reality>

Hagggle Traces (Trace1/ Trace2/ Trace3):

<http://crowdad.cs.dartmouth.edu/meta.php?name=cambridge/hagggle>

National University of Singapore Trace:

<http://crawdad.cs.dartmouth.edu/meta.php?name=nus/contact>

Bluetooth trace in Utoronto:

<http://www.cs.toronto.edu/~stefan/downloads/>

This work is joint effort with Andrew Miklas, and Stefan Sariou.

References

[A Preliminary Investigation of Worm Infections in a Bluetooth Environment](#). Jing Su, Kelvin K. W. Chan, Andrew G. Miklas, Kenneth Po, Ali Akhavan, Stefan Sariou, Eyal de Lara, Ashvin Goel. WORM 2006.